Scientific Annals of Economics and Business
70 (3), 2023, 379-398
DOI: 10.47743/saeb-2023-0028

Resilience to Online Privacy Violation: Developing a Typology of Consumers

Jelena Budak*, Edo Rajh, Bruno Škrinjarić*****

Abstract: This study examines which segments of population with similar resilience to online privacy violation, severity of online privacy violation, and attitudes towards online privacy concern exist in Croatia, and whether they can be differentiated by demographic characteristics and attitudes towards other online constructs. Research is performed on a representative sample of Croatian Internet users who experienced online privacy violation. The survey data were analyzed using factor analysis, k-means cluster analysis, chi-square test and ANOVA. The findings indicate three groups of consumers with: (1) low-resilience, (2) moderate-resilience, and (3) high-resilience; who differ in age, income, and online buying habits.

Keywords: resilience; online privacy violation; privacy concern; consumer typology; Croatia.

JEL classification: D12, D91.

* Institute of Economics, Zagreb, Zagreb, Croatia; e-mail: *jbudak@eizg.hr* (corresponding author).
** Institute of Economics, Zagreb, Zagreb, Croatia; e-mail: *erajh@eizg.hr*.
*** Institute of Economics, Zagreb, Zagreb, Croatia; e-mail: *bskrinjaric@eizg.hr*.

Article history: Received 28 June 2022 | Accepted 15 July 2023 | Published online 21 September 2023

To cite this article: Budak, J., Rajh, E., Škrinjarić, B. (2023). Resilience to Online Privacy Violation: Developing a Typology of Consumers. *Scientific Annals of Economics and Business*, 70(3), 379-398. https://doi.org/10.47743/saeb-2023-0028.

1. INTRODUCTION

Online activities take an increasing part in almost all aspects of everyday life in the digital era. In time of pandemics consumers turn even more to online shopping, e-banking, e-learning, e-government services, and other online services for the sake of convenience, accessibility, and safety (Das *et al.*, 2021). This increase in the volume of online activities also carries certain privacy risks and raises privacy concerns (Liao *et al.*, 2011; Baek *et al.*, 2014; Bansal & Zahedi, 2015; Ginosar & Ariel, 2017; Anić *et al.*, 2019; Škrinjarić *et al.*, 2019). The neglected aspect of online privacy violation studies is how Internet users cope with this stressful event. Preliminary survey data for Internet users in Croatia reveal that an average consumer recovers rather quickly after subjectively experiencing online privacy violation (Škrinjarić *et al.*, 2019). Assuming there are some statistical differences in the level of resilience among different socio-demographic groups, a more in-depth analysis is needed to better understand the interrelationship between socio-demographic characteristics and consumer resilience to online privacy violation.

The objective of this study is to investigate consumers' resilience to online privacy violation associated with their level of online privacy concern and with the perceived severity of the privacy violation incident. It provides new insights in the typology of consumers who had recently experienced online privacy violation by finding evidence-based answers to the following research questions: (1) Can consumers be segmented into distinct groups based on the resilience to online privacy violation?; and, if so, (2) What common characteristics are shared among members of each cluster?; and (3) Are there differences in these groups based on the demographics, online buying behavior and attitudes of consumers in each cluster?

This research contributes to literature in several ways. Firstly, the increased rate of digitalization, which in turn increases the need for large amount of (individual) information to be available online, raises the opportunity of various online privacy violations. Hence, governments, private firms, researchers, and everyday consumers are paying more attention to effects of these adverse events, especially in increasing resilience to such attacks. Stakeholders might face the dilemma of increasing in general Internet users' resilience to online privacy infringements or e.g., of educating the already quite resilient Internet users to nonetheless care about preserving their privacy when online. Debate on these ethical issues is important, yet beyond the scope of this study.

Secondly, online privacy has recently gained importance, especially since the introduction of General Data Protection Regulation (GDPR). Governments and businesses are shaping their strategies to be in line with these regulations and to improve security for their online services. Finally, this research presents an important novelty since it combines "privacy" and "resilience" concepts to the analysis of consumers in an online environment. This is particularly important, given that both concepts originated outside of the social domain, and have, to the best of our knowledge, not yet been analyzed in digital environment. This study has elements of interdisciplinary online privacy research as suggested by Ginosar and Ariel (2017) and adds value to the existing knowledge.

The remainder of our paper is structured as follows. Section 2 provides a short literature review on variables used to explain the typology of online consumers, followed by Section 3 with the survey data and methodology. The results of the empirical analysis are presented and discussed in Section 4. Section 5 concludes on findings and implications and suggests directions for future research.

2. LITERATURE REVIEW

This research incorporates intertwined concepts of privacy concern, privacy violation and resilience, all in an online environment and focused on consumers who use Internet. In the core of the research lies resilience – a complex multifaceted concept used in different research disciplines (Brand & Jax, 2007; Bhamra *et al.*, 2011; Herrman *et al.*, 2011). Among many definitions (Martin-Breen & Anderies, 2011), consumers resilience to online privacy violation incident might be defined according to B. W. Smith *et al.* (2008) as the ability of an individual to "bounce back", i.e., to successfully recover from a stressful situation.

Online privacy concern can be defined as individuals' apprehension and uneasiness over the use of their personal data (Lwin *et al.*, 2007), and it reflects the level of discomfort felt by an individual when using the Internet. Consumers who experienced online privacy violation have more privacy concerns (Xu *et al.*, 2011; Afolabi *et al.*, 2021). Besides feeling concerned, consumers might feel more frustrated by incidents that have severe consequences. It is therefore reasonable to assume that consumers who are more concerned about their online privacy might be less resilient to online privacy violations. Here the subjective assessment of privacy breach seriousness plays a crucial role in the individual adaptation and recovery process (Calo, 2011; Bansal & Zahedi, 2015).

To explain differences in the typology of consumers, a set of attributes was included in the cluster analysis. Past research evidence is in favor of including socio-demographic characteristics of consumers (Kaapu & Tiainen, 2009). However, in the face of massive Internet usage and increasing number of 'digital natives' (Reed, 2014), contemporary studies do not provide a clear-cut socio-demographic picture of consumer profile and online behavior. Earlier studies on socio-demographic characteristics of online consumers showed they are likely to be older, better educated, and have a higher income (Graeff & Harmon, 2002; Swinyard & Smith, 2003). The influence of personality types of Internet users to their Internet usage motives and online activities has been confirmed as well (Bubaš & Hutinski, 2006). More recent studies are not so conclusive, at least about the impact of gender on the use of Internet and online commerce purchasing (Akman & Rehan, 2014). However, different age groups may have different tendencies towards online purchasing (Hwang *et al.*, 2006).

Consumer behavior literature and more recent research exploring online consumer behavior deal with online shopping (Islam, 2019), e-commerce (Oliveira & Toaldo, 2015), and m-commerce (Sharif *et al.*, 2014). On the other hand, studies include more specific aspects in the analysis (Dennis *et al.*, 2009), such as online privacy concern (Anić *et al.*, 2019). Research findings show that both privacy concerns and previous privacy violations stand as an obstacle to the growth of e-commerce (Miyazaki & Fernandez, 2001) by inhibiting more customers from engaging in e-commerce (Lee, 2002; Pavlou & Fygenson, 2006). Although privacy stands as a major concern for online purchasers (Lee, 2002), the skeptical attitude towards online shopping could be mitigated by customer positive experience (Soopramanien, 2011). Balancing between protecting privacy and providing benefits for consumers is a significant challenge for companies because consumers ask for personalized services but resist collecting personal information (Awad & Krishnan, 2006). Privacy paradox and privacy calculus (J. H. Smith *et al.*, 2011) seem to considerably determine the behavior of consumers and need to be addressed carefully in business policies as well. Consumers would voluntarily give away some privacy and disclose personal information in exchange for the benefits of using online services. Enduring privacy violation online might impact their individual privacy calculus and

consequently affect online consumer online (Xu *et al.*, 2011). Rare studies of consumer resilience indicate that level of resilience differently affects consumer attitudes (Rew & Minor, 2018) and purchasing outcomes (Kursan Milaković, 2021) wherein the online privacy violation context has not been regarded.

3. DATA AND METHODOLOGY

3.1 Survey Data

This research is based on the survey data on Internet users in Croatia who reported to having experienced online privacy violation in a period of three years prior to the survey. The target population were Internet users in Croatia aged 18 years old or older. The sample structure was determined according to the Eurobarometer 91.1 (European Commission, 2023). The sample was two-way stratified by region and settlement size.

The survey questionnaire, developed by the co-authors, had two filter conditions. Firstly, potential respondents had to be an Internet user; and, secondly, had to have experienced privacy violation on the Internet in the last three years. The sampling quota required that at least 66% of respondents are consumers who engage in buying online while the remaining one third do not purchase online but search online catalogues, use e-banking services, social networks and perform other activities on the Internet.

The fieldwork was conducted using Computer Assisted Telephone Interviewing (CATI) in the period from January to February 2021. The response rate was 4.6% and the net sample consists of 1,000 Internet users who experienced online privacy violation (sample characteristics are presented in Table no. A1).

3.2 Empirical Methodology

The first stage of data analysis included techniques for scale reliability and validity assessment of latent constructs used in our study. Within this stage we used Cronbach's alpha (CA) and Alpha-if-deleted coefficients, and exploratory and confirmatory factor analysis techniques. CA coefficient is used as a measure of scale reliability because it measures internal consistency, that is, how closely related a set of items is as a group. Alpha-if-deleted coefficient is used for measuring the internal consistency of the scale. The dimensionality of the scale is tested by exploratory and confirmatory factor analysis with measurement models where each manifest variable only loads on one latent variable, and with the assumption of the independence of measurement errors (Kline, 1998).

The second stage of data analysis included K-means cluster analysis which was employed to determine the specific groups within the population with similar attitudes. Finally, the third stage of data analysis was oriented towards identifying the differences among the groups of respondents. The differences were tested using the chi-square test and ANOVA.

3.3 Description of Variables used

Latent constructs in our analysis include resilience to online privacy concern (RES), online privacy concern (OPC), online privacy awareness (OAW), Internet benefits (BNF), digitalization anxiety (DA) and protective behavior (PB).

Measurement scale to assess resilience (RES) was adapted from Brief Resilience Scale (BRS) developed by (B. W. Smith *et al.*, 2008). Two features of the BRS were in favor of choosing this scale. Firstly, BRS contains only six items to be incorporated in the large telephone survey; and secondly, it was originally developed to measure resilience of adults who were the surveyed population in this research as well. BRS statements were adapted to measure resilience to the online privacy violation after the most recent incident. Items 2, 4 and 6 indicate the reverse direction of actions from items 1, 3 and 5. The appropriateness of the adapted BRS as measurement scale was tested and its psychometric characteristics were found appropriate (Rajh *et al.*, 2021). It is important to emphasize that our survey examines the citizens' *subjective* assessment of privacy violation in an online environment, which does not necessarily need to coincide with the definition of privacy violation.

To measure online privacy concern (OPC), three constructs originating from the six-item online privacy concern scale developed by H. J. Smith *et al.* (1996) were borrowed. They cover different aspects of personal online privacy concern: general concern about online privacy, concern about information collection and about privacy violation when using Internet.

Online privacy awareness (OAW) was measured using three items adopted from Xu *et al.* (2008) and Malhotra *et al.* (2004). Online privacy awareness reflects the level of individual's awareness about the importance of online privacy and possibilities that some information and data could be used without owners' consent. Online privacy awareness is higher for respondents who have knowledge about privacy issues and the solutions employed by companies and governments to ensure privacy. Further, privacy awareness is higher for respondents consider that web sites seeking information online should disclose the way the data are collected, processed, and used. In addition, the level of online privacy awareness is higher if individuals consider that a good online privacy policy should have a clear and conspicuous disclosure.

Digitalization anxiety (DA) can be defined as the tendency of individuals to be uneasy, apprehensive, or fearful about the increasing pace of digitalization, the loss of data and possible mistakes of using the computers (Cazan *et al.*, 2016). Although some studies did not find significant relationship between DA and information privacy concern (Korzaan & Boswell, 2008), other studies indicate that individuals who experience high levels of DA behave less comfortably around computers and exhibit higher levels of privacy concern (Škrinjarić *et al.*, 2018).

Measures for protective behaviors (PB) were adopted from Lwin *et al.* (2007) and adapted to our specific context. These behaviors are motivated by the individuals' need to protect sensible personal information. Lwin *et al.* (2007) stated that protective behavior implies personal information fabrication, withholding and protecting by using privacy enhancing technologies. Their results suggest that firms and regulators need to be perceived by consumers as acting responsibly in their utilization of personal data if they wish to avoid negative behavioral responses by consumers.

To control the consumers' intrinsic motivation for using the Internet, perceived benefits of using the Internet (BNF) from Dinev and Hart (2006) were also included in the model. Previous research found that Internet users develop rules of information disclosure by evaluating the perceived risks and benefits to manage their privacy effectively (Petronio, 1991). Past research also confirmed that perceived benefits have an impact on information disclosing intention (Dinev & Hart, 2006; Li, 2011). Perceived benefits through intentions

affect actual behavior, which means that individuals will reduce their tendency to engage in Internet protective behavior (Li, 2011).

Items used to measure these latent constructs are presented in Table no. A2. Answers to what extent a respondent agrees with the item statements were given at 5-point Likert scale ranging from 1 - Strongly disagree to 5 - Strongly agree.

Finally, our study also includes directly observed variables. Privacy violation seriousness (PV_ser) is measured by assessing subjective evaluation of how severe the experienced privacy incident was for the respondent. The straightforward individual answers to 'How serious was this case of online privacy violation for you?' were recorded on the scale from 1 – *Negligibly serious* to 5 – *Very serious*. General Internet attitude scale (GIAS) is also a single-item variable. This item is adapted from one item of the attitude scale of the theory of planned behavior (Ajzen, 1991; Yoon, 2011). Description of all variables used in this research is presented in Table no. A3.

4. RESULTS

4.1 Descriptive Statistics

Privacy violation instances experienced by sampled Internet users were reported as answers to an open-ended question, which were then grouped into six respective categories of privacy violations (Figure no. 1). In the content analysis we employed inductive (open) coding where categories are 'data-driven' i.e., constructed *a posteriori* based on the actual content of survey responses (Popping, 2015; Lune & Berg, 2017; Vears & Gillam, 2022).

Almost half of privacy violation cases refer to receiving unwanted advertisements and commercials after visiting a website. The second most common type of online privacy violation was recording one's location, conversations, Internet searches and messages.

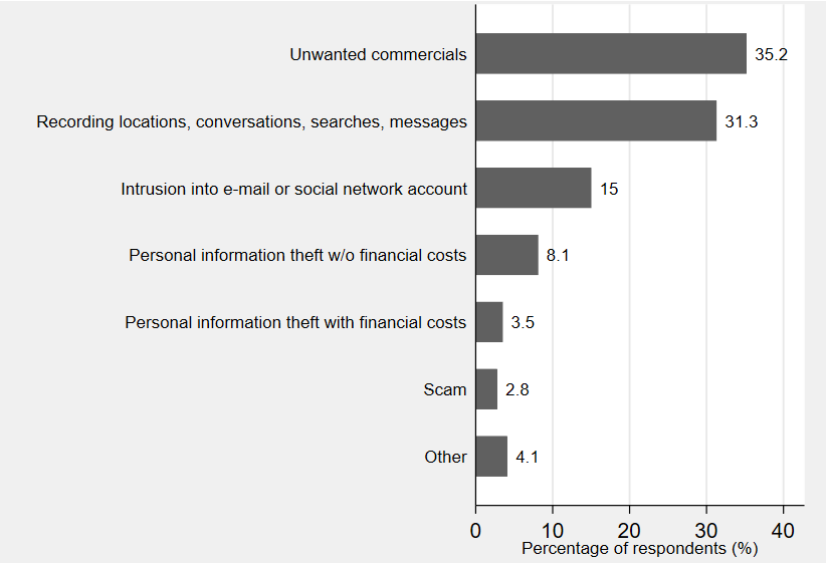

Figure no. 1 – Privacy violation online cases

After naming and describing a form of their online privacy violation, respondents also gave their subjective assessment of the "seriousness" of this privacy violation on the Likert scale with scores ranging from 1 - *Negligibly serious* to 5 - *Very serious*. For each different group of online privacy violation cases, we calculated the average of this subjective assessment of the severity of the violation (Figure no. 2). While unwanted commercials are the most common form of online privacy violation, it poses the least serious problem for Internet users. As expected, the most serious violations are those including the theft of personal data with financial costs, but fortunately, they are also among the rarest ones.

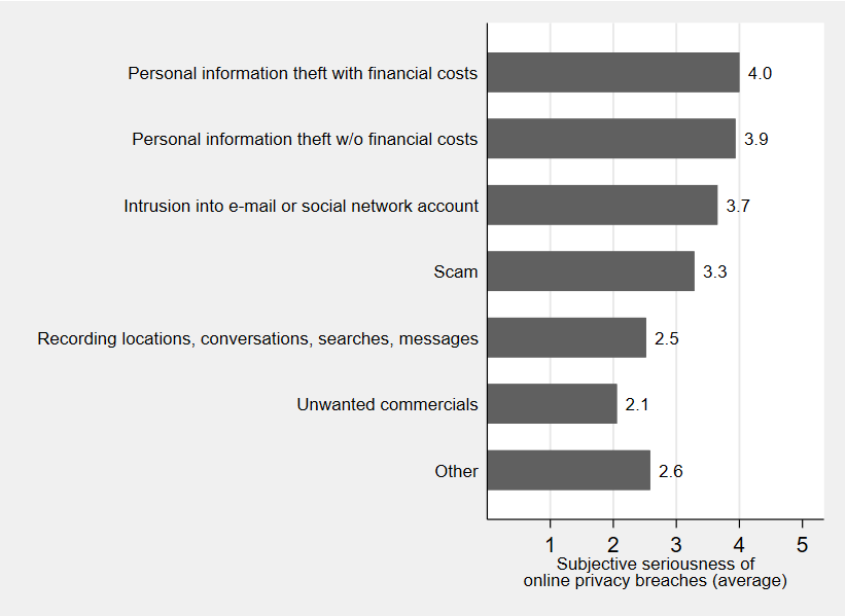

Figure no. 2 – Perceived severity of online privacy violations

Descriptive statistics used to measure latent constructs are presented in Table no. 1. Internet users on average have a certain level of resilience to online privacy violation. For most respondents, it didn't take much time to recover from the most recent online privacy violation incident (res_3 = 3.32). In fact, they reported they came through the most recent online privacy violation incident with little trouble (res_5 = 3.55). These findings are in line with the prevalence of "soft" privacy violation cases and their perceived low severity. On the other hand, Internet users are on average concerned about their privacy when online, which is in line with past research (Anić *et al.*, 2019). A major concern is reported about extensive collection of personal information over the Internet (opc_2 = 3.69). Regarding online privacy awareness, consumers are not up to date with privacy issues and solutions offered on the market (oaw_1 = 2.85), while on the other hand, they agree that web sites should be clear about their data-gathering policies (oaw_3 = 4.31) and how this information is used (oaw_2 = 4.12). Most of sampled consumers feel that digitalization is a threat to privacy (da_1 = 3.45), but they are also somewhat willing to forego their online privacy concerns if the need for obtaining a certain piece of information is high (bnf_1 = 3.34).

Finally, concerning protective behavior, most consumers employ tactics of refusing to provide personal information to untrustworthy websites (pb_6 = 3.91) and only filling out data partially when registering to certain web sites (pb_3 = 3.27).

Table no. 1 – Latent construct item descriptive statistics

Latent construct	Item	Mean	St. dev.	Min.	Max.
Resilience to online privacy violation (RES)	res_1	2.93	1.22	1	5
	res_2	2.57	1.23	1	5
	res_3	3.32	1.21	1	5
	res_4	2.41	1.18	1	5
	res_5	3.55	1.16	1	5
	res_6	2.24	1.20	1	5
Online privacy concern (OPC)	opc_1	3.31	1.03	1	5
	opc_2	3.69	1.08	1	5
	opc_3	3.51	1.07	1	5
Online privacy awareness (OAW)	oaw_1	2.85	1.05	1	5
	oaw_2	4.12	1.07	1	5
	oaw_3	4.31	0.88	1	5
Internet benefits (BNF)	bnf_1	3.34	0.98	1	5
	bnf_2	2.92	1.03	1	5
Digitalization anxiety (DA)	da_1	3.45	1.09	1	5
	da_1	2.99	1.15	1	5
Protective behavior (PB)	pb_1	2.08	1.09	1	5
	pb_2	2.05	1.22	1	5
	pb_3	3.27	1.27	1	5
	pb_4	3.17	1.25	1	5
	pb_5	2.49	1.29	1	5
	pb_6	3.91	1.25	1	5

Note: "St. dev." denotes standard deviation.

4.2 Latent Construct Estimation

Table no. 2 presents the CA coefficients and item correlations for all items used to estimate latent constructs. Regarding the RES variable, a CA coefficient value of 0.8962 and the results of the measurement scale reliability analysis indicate that the measurement scale used in constructing the RES variable possesses a satisfactory level of reliability. Both analyzed types of correlations indicate a high degree of correlation of each statement with the overall measurement scale, while Alpha-if-deleted values indicate that in this case the removal of any statement would cause a decrease in CA coefficient, i.e., the scale would become less reliable. A similar argument is used when deciding to keep all the items for OPC variable, as removal of any item would decrease the CA coefficient value of 0.7679. The story is somewhat different for OAW variable, where the alpha-if-deleted value for the first item (oaw_1) indicates that CA coefficient would increase from 0.3244 to 0.5846. Based on this result, we proceeded without item *oaw_1* to estimate the OAW variable. The same is true for item pb_6, whose removal would marginally increase CA coefficient from 0.7375 to 0.7381.

Table no. 2 – Item correlations and Cronbach alphas

Latent construct	Item	Inter-item correlation	Item-rest correlation	Cronbach alpha	Alpha-if-deleted
Resilience to online privacy violation (RES)	res_1	0.6101	0.6623	0.8962	0.8867
	res_2	0.5828	0.7398		0.8748
	res_3	0.6129	0.6543		0.8879
	res_4	0.5746	0.7637		0.8710
	res_5	0.5799	0.7484		0.8734
	res_6	0.5787	0.7516		0.8729
Online privacy concern (OPC)	opc_1	0.5281	0.5964	0.7679	0.6912
	opc_2	0.5499	0.5798		0.7096
	opc_3	0.4927	0.6239		0.6602
Online privacy awareness (OAW)	oaw_1	0.413	0.0006	0.3244	0.5846
	oaw_2	0.0437	0.2563		0.0837
	oaw_3	-0.0427	0.3301		0.0005
Internet benefits (BNF)	bnf_1 bnf_2	0.2907		0.4505	
Digitalization anxiety (DA)	da_1 da_1	0.3740		0.5444	
Protective behavior (PB)	pb_1	0.3094	0.5002	0.7375	0.6914
	pb_2	0.2899	0.5687		0.6712
	pb_3	0.3122	0.4908		0.6941
	pb_4	0.349	0.3691		0.7283
	pb_5	0.2861	0.5821		0.6671
	pb_6	0.3603	0.3331		0.7381

EFA was conducted to test convergent validity of measurement scales for each latent construct, as well as to preliminary test their dimensionality. The principal component was used as a method of factor extraction and Kaiser-Guttman rule (specifying that factors with eigenvalues greater than 1 are retained) was used as a method for determining the number of extracted factors (Table no. 3A). Results indicate that measurement scales for all our latent variables are unidimensional, as all items have high factor loadings on their respective factor (Table no. 3B). EFA results also indicate that latent variable scales pose the attribute of convergent validity. Therefore, the initial set of selected items can be considered as one measurement scale for each of those variables.

Table no. 3 – Exploratory factor analysis results

Panel A: Eigen values

Factor	Eigen values	Cumulative eigen values	Percentage of explained variance	Cumulative percentage of explained variance
1	5.0116	5.0116	0.2278	0.2278
2	2.6823	7.6939	0.1219	0.3497
3	2.0323	9.7262	0.0924	0.4421
4	1.5299	11.2562	0.0695	0.5116
5	1.3037	12.5598	0.0593	0.5709
6	1.1031	13.6629	0.0427	0.6136
7	0.8446	14.5075	0.0384	0.6520
8	0.7902	15.2977	0.0359	0.6879
9	0.7433	16.0410	0.0338	0.7217

Factor	Eigen values	Cumulative eigen values	Percentage of explained variance	Cumulative percentage of explained variance
10	0.6714	16.7124	0.0305	0.7522
11	0.6509	17.3633	0.0296	0.7818
12	0.6092	17.9725	0.0277	0.8095
13	0.5657	18.5383	0.0257	0.8352
14	0.5616	19.0999	0.0255	0.8607
15	0.5348	19.6346	0.0243	0.8850
16	0.4905	20.1251	0.0223	0.9073
17	0.4523	20.5775	0.0206	0.9279
18	0.4224	20.9999	0.0192	0.9471
19	0.3977	21.3976	0.0181	0.9652
20	0.3838	21.7814	0.0174	0.9826
21	0.2176	21.9990	0.0099	0.9925
22	0.1651	22.1641	0.0075	1.0000

Panel B: Eigen vectors

Latent construct	Item	F1	F2	F3	F4	F5	F6
Resilience to online privacy violation (RES)	res_1	0.7352					
	res_2	0.7981					
	res_3	0.7678					
	res_4	0.8357					
	res_5	0.8317					
	res_6	0.8325					
Online privacy concern (OPC)	opc_1		0.7037				
	opc_2		0.7010				
	opc_3		0.6976				
Online privacy awareness (OAW)	oaw_1				-		
	oaw_2				0.766		
	oaw_3				0.730		
Internet benefits (BNF)	bnf_1					0.694	
	bnf_2					0.697	
Digitalization anxiety (DA)	da_1						0.670
	da_1						0.671
Protective behavior (PB)	pb_1			0.727			
	pb_2			0.806			
	pb_3			0.546			
	pb_4			0.514			
	pb_5			0.762			
	pb_6			-			

Notes: Principal factor method was used, and factors were rotated using orthogonal varimax rotation. Factor loadings lower than 0.5 were dropped and are not reported ("-").

Convergent validity was also assessed with CFA, where we tested two models: (1) model with all items for all latent variables; and (2) model using only items with positive direction for RES variable, and without items *oaw_1* and *pb_6* for OAW and PB variables. CFA results, presented in Table no. 4, further confirm EFA results. Fit indices show that measurement Model 2 has an acceptable level of fit to empirical data. Hence, in all further analysis RES variable will be based only on items with positive direction (*res_1*, *res_3* and *res_5*), OAW variable will be based on items *oaw_1* and *oaw_2*, and item *pb_6* will not be

used for PB variable. All analyzed items load on their respective factors and all loadings are statistically significant. Thus, results indicate that all scales are unidimensional.

Table no. 4 – Confirmatory factor analysis results

	Model 1	Model 2
Resilience (RES)		
res_1	1.000 (-)	1.000 (-)
res_2	1.124*** (0.048)	-
res_3	0.981*** (0.049)	1.027*** (0.059)
res_4	1.116*** (0.049)	-
res_5	1.093*** (0.048)	1.121*** (0.064)
res_6	1.161*** (0.051)	-
Online privacy concern (OPC)		
opc_1	1.000 (-)	1.000 (-)
opc_2	1.003*** (0.058)	1.005*** (0.058)
opc_3	1.119*** (0.063)	1.119*** (0.064)
Online privacy awareness (AOW)		
oaw_1	1.000 (-)	-
oaw_2	-14604.33 (35526.89)	1.000 (-)
oaw_3	-8086.436 (19687.9)	0.631*** (0.139)
Internet benefits (BNF)		
bnf_1	1.000 (-)	1.000 (-)
bnf_2	1.129*** (0.242)	1.112*** (0.216)
Digitalization anxiety (DA)		
da_1	1.000 (-)	1.000 (-)
da_1	1.032*** (0.093)	1.034*** (0.094)
Protective behavior (PB)		
pb_1	1.000 (-)	1.000 (-)
pb_2	1.201*** (0.067)	1.200*** (0.065)
pb_3	0.948*** (0.071)	0.851*** (0.066)
pb_4	0.737*** (0.069)	0.689*** (0.066)
pb_5	1.261*** (0.077)	1.217*** (0.074)
pb_6	0.606*** (0.068)	-
N	1,000	1,000
Chi-squared	7435.139***	4041.444***
RMSEA	0.152	0.055
CFI	0.871	0.920
TLI	0.821	0.974
GFI	0.866	0.982

Notes: (***) denotes significance level p<0.01. Standard errors are in parentheses.
RMSEA = Root mean square error of approximation, CFI = Comparative fit index,
TLI = Tucker-Lewis index, GFI = Goodness of fit index.

4.3 Typology of Consumers

The next step in the analysis was the classification of consumers according to their resilience to online privacy concern. K-means cluster analysis was employed to classify consumers based on three online privacy related variables: seriousness of privacy violation

incidents, online privacy concern of consumers and consumers' resilience to online privacy violation. Elbow method was used as a criterion for determining the optimal number of clusters in a dataset. Mean values were calculated for RES and OPC variable-items and these mean values were taken as an input in the K-means cluster analysis. Since privacy violation seriousness (PV_ser) is measured using a single-item scale, its original values were taken as an input in the K-means cluster analysis. Results of the K-means cluster analysis differentiated three homogeneous segments of consumers (Table no. 5 and Figure no. 3).

Table no. 5 – K-means cluster analysis results

	Total sample (n = 1,000)	**Cluster 1 (n = 283)**	**Cluster 2 (n = 406)**	**Cluster 3 (n = 311)**	**ANOVA**
Privacy violation seriousness	2.7	4.5	2.5	1.3	F = 2,274.6***
Online privacy concern	3.5	3.9	3.7	2.8	F = 170.6***
Resilience to online privacy violation	3.3	2.4	3.3	4.1	F = 383.4***

Note: (***) denote significance level p<0.01.

Cluster 1 (Low Resilience) is a low resilience cluster with the lowest value of RES variable. Consumers in this cluster, according to their subjective assessment, have experienced quite serious online privacy violations (mean value 4.5). These consumers also exhibit the highest level of online privacy concern.

Cluster 2 (Moderate Resilience) is a medium resilience cluster. Consumers in this cluster have experienced online privacy violations that are considerably less serious than those experienced by consumers from cluster 1. However, consumers in this segment still exhibit relatively high levels of online privacy concern.

Cluster 3 (High Resilience) is a high resilience cluster. Consumers in this cluster have experienced online privacy violations that are the least serious of all three clusters. Also, when compared to consumers from other clusters, consumers in this cluster exhibit the lowest levels of online privacy concern.

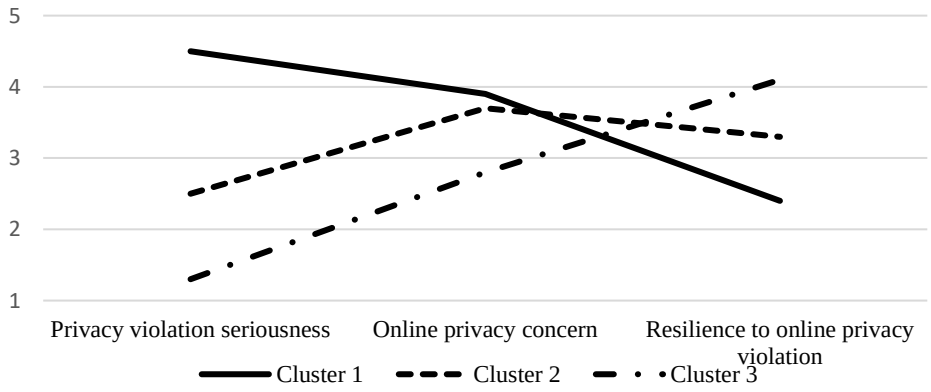

Figure no. 3 – K-means cluster analysis results

4.4 Differences among groups of consumers

Next, we examine the differences among the identified clusters based on the demographic characteristics and attitudes of member consumers (Table no. 6 and Table no. 7).

Table no. 6 – Differences in demographics among clusters (relative frequencies, %)

	Total sample (n = 1,000)	Cluster 1: Low Resilience (n = 283)	Cluster 2: Moderate Resilience (n = 406)	Cluster 3: High Resilience (n = 311)	Chi-squared test statistic
Gender					
Male	48.7	45.9	51.7	47.3	2.607
Female	51.3	54.1	48.3	52.7	
Age					
18-34	34.7	36.8	35.0	32.5	
35-50	30.4	35.3	28.6	28.3	9.868**
51+	34.9	27.9	36.5	39.2	
Education					
Secondary school or less	53.8	55.8	52.7	53.4	0.686
Some level of higher education	46.2	44.2	47.3	46.6	
Monthly household income					
Up to 6,500 HRK [a]	23.4	21.5	23.2	25.5	
6,501-10,000 HRK	29.5	23.7	33.7	29.2	19.867***
10,001-15,000 HRK	32.6	43.8	27.6	28.8	
More than 15,000 HRK	14.5	11.0	15.6	16.5	
Shopping on Internet					
Yes	66.7	52.7	71.2	73.6	35.555***
No	33.3	47.3	28.8	26.4	

Notes: (**), (***) denote significance levels $p<0.05$ and $p<0.01$, respectively. Pearsons' Chi-squared statistic was used. Due to missing data, for monthly household income N = 777. [a] 1 EUR ~ 7.5 HRK.

There are statistically significant differences among identified clusters considering age, monthly household income and their previous involvement in online buying. There are no statistically significant differences in gender and the level of education.

Members of Cluster 1 (Low Resilience) are dominantly young consumers whose low resilience is in line with their high privacy concern and the highest perceived seriousness of the privacy violation incident they had experienced. These Internet users employ some protective measures and have a high digitalization anxiety which at first sight, contrasts with their digital native nature. However, the strongest negative experience with online privacy violation explains these characteristics and the perceived low benefits of using Internet. It might as well be that this rather high-income group of a younger age is taking Internet benefits as granted. Intensive Internet usage could also increase their fear of losing the data and making mistakes when working on computer or being online. This distress is one aspect of being anxious about going digital.

The age composition of Cluster 2 (Moderate Resilience) is in line with the average of the whole sample. Nevertheless, Cluster 2 is the most interesting group. Consumers showed moderate resilience and lower perceived levels of severity of the privacy violation incident. Despite some extent of online privacy concern and general negative attitude towards Internet, they keep on practicing e-commerce/shop online. Most likely they see advantages

of the Internet and therefore balance between perceived costs in terms of privacy violation risk and benefits of services and activities offered online.

Members of Cluster 3 (High Resilience) are dominantly older consumers aged over 51. In Cluster 3, the proportion of consumers with either the highest or the lowest income is above the entire sample average. The high resilience to online privacy violation is in line with the lowest perceived seriousness of the incident experienced. Cluster members are not privacy concerned, have positive attitudes towards Internet and no digitalization anxiety. It is not surprising they see many benefits of Internet as many of them regularly engage in e-commerce/shop online.

Table no. 7 – Differences in attitudes among clusters (means)

	Total sample (n = 1,000)	**Cluster 1: Low Resilience (n = 283)**	**Cluster 2: Moderate Resilience (n = 406)**	**Cluster 3: High Resilience (n = 311)**	**ANOVA F-statistic**
Online privacy awareness	3.76	3.78	3.76	3.74	0.336
General Internet attitude scale	3.79	3.75	3.70	3.95	8.939***
Internet benefits	3.13	2.98	3.12	3.29	11.329***
Digital anxiety	3.22	3.47	3.33	2.84	42.767***
Protective behavior	2,83	3,00	2,94	2,53	32.547***

Note: (***) denote significance levels p<0.01.

5. CONCLUSIONS

The findings on the typology of Internet users who experienced Internet privacy violation differentiated three groups of consumers (low-resilience, moderate-resilience, and high-resilience) that are homogeneous within group and heterogeneous between identified groups for all three analyzed variables. The typology is based on the respondents' online privacy concern, their subjective assessment of the severity of privacy violation and their resilience to it. These are novel aspects included in consumer behavior online research.

A self-reported measure of concern about online privacy and a subjective notion of severity of privacy violation incident seem to be closely associated to the consumer's resilience to online privacy violation incident. Additionally, consumers who perceive positive outcomes of using Internet would recover faster or cope easier with the privacy violation event. Here the most interesting finding is that even moderately resilient consumers do not sustain e-buying. Surprisingly, older customers belong to the high-resilience cluster, suggesting that other personal characteristics might affect their behavior. Their longer life experience might prevent them from dramatically reacting to online privacy violation. On the other side, younger generations are highly sensitive to privacy breaches and show a higher rate of digitalization anxiety. They therefore employ more protective measures online. Low resilience of upcoming generations of consumers calls for an increased attention of marketers and business policies in general as well as for better communication of privacy protection regulations.

This study is not without limitations. First, although the notion of resilience is a very broad term appearing in various domains, it was not possible to include all theoretical contributions of resilience in this paper. Even though our dataset contains a representative sample of citizens over the age of 18, children begin to be active online from an early age, and

their level of resilience may differ from that of the older population. Likewise, the measured level of resilience certainly changes over time as technology advances, so the time component should certainly be included in future research. This model is set to analyze online privacy violation breach effects on citizens' attitudes towards various digital public services (via their degree of resilience). However, this adverse event may also have spillover effects to citizens' closer circle of relatives and friends, which are currently not included in the model. Our dataset is "cross-section" type, as opposed to panel structure, so the results can be interpreted only in terms of correlations or associations, and not causations. Finally, the model is tested on citizens of one country in specific socio-cultural and economic conditions, and without additional empirical verification it cannot be generalized outside these conditions.

Funding

This work has been fully supported by the Croatian Science Foundation under the Project IP-2019-04-7886.

References

Afolabi, O. O., Ozturen, A., & Ilkan, M. (2021). Effects of privacy concern, risk, and information control in a smart tourism destination. *Economic Research-Ekonomska Istraživanja, 34*(1), 3119-3138. http://dx.doi.org/10.1080/1331677X.2020.1867215

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

Akman, I., & Rehan, M. (2014). Online purchase behaviour among professionals: A socio-demographic perspective for Turkey. *Economic Research-Ekonomska Istraživanja, 27*(1), 689-699. http://dx.doi.org/10.1080/1331677X.2014.975921

Anić, I. D., Budak, J., Rajh, E., Recher, V., Škare, V., & Škrinjarić, B. (2019). Extended model of online privacy concern: What drives consumers' decisions? *Online Information Review, 43*(5), 799-817. http://dx.doi.org/10.1108/OIR-10-2017-0281

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly, 30*(1), 13-28. http://dx.doi.org/10.2307/25148715

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31*, 48-56. http://dx.doi.org/10.1016/j.chb.2013.10.010

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62-77. http://dx.doi.org/10.1016/j.dss.2015.01.009

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375-5393. http://dx.doi.org/10.1080/00207543.2011.563826

Brand, F. S., & Jax, K. (2007). Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. *Ecology and Society, 12*(1), 23. http://dx.doi.org/10.5751/ES-02029-120123

Bubaš, G., & Hutinski, Z. (2006). Conceptual model, potential predictors and dimensions of affinity for the use of the Internet. . *Drustvena istrazivanja, 12*(1), 27-44.

Calo, R. M. (2011). The Boundaries of Privacy Harm. *Indiana Law Journal, 86*(3), 1131-1162.

Cazan, A. M., Cocoradă, E., & Maican, C. I. (2016). Computer anxiety and attitudes towards the computer and the internet with Romanian high-school and university students. *Computers in Human Behavior, 55*(Part A), 258-267. http://dx.doi.org/10.1016/j.chb.2015.09.001

Das, G., Jain, S. P., Maheswaran, D., Slotegraaf, R. J., & Srinivasan, R. (2021). Pandemics and marketing: Insights, impacts, and research opportunities. *Journal of the Academy of Marketing Science, 49*, 835-854. http://dx.doi.org/10.1007/s11747-021-00786-y

Dennis, C., Merrilees, B., Jayawardhena, C., & Tiu Wright, L. (2009). E-consumer behavior. *European Journal of Marketing, 43*(9/10), 1121-1139. http://dx.doi.org/10.1108/03090560910976393

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. http://dx.doi.org/10.1287/isre.1060.0080

European Commission. (2023). *Eurobarometer 91.1* (ZA7561). Retrieved from GESIS: https://search.gesis.org/research_data/ZA7561?doi=10.4232/1.13317

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management, 54*(7), 948-957. http://dx.doi.org/10.1016/j.im.2017.02.004

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318. http://dx.doi.org/10.1108/07363760210433627

Herrman, H., Stewart, D. E., Diaz-Granados, N., Berger, E. L., Jackson, B., & Yuen, T. (2011). What is resilience? *The Canadian Journal of Psychiatry, 56*(5), 258-265. http://dx.doi.org/10.1177/070674371105600504

Hwang, W., Jung, H. S., & Salvendy, G. (2006). Internationalisation of e-commerce: A comparison of online shopping preferences among Korean, Turkish and US populations. *Behaviour & Information Technology, 25*(1), 3-18. http://dx.doi.org/10.1080/01449290512331335636

Islam, S. (2019). Factors Influencing Customer's Intention to Adopt Online Shopping: A Holistic Approach. *International Journal of Business and Technopreneurship, 9*(1), 57-66.

Kaapu, T., & Tiainen, T. (2009). Consumers' Views on Privacy in E-Commerce. *Scandinavian Journal of Information Systems, 21*(1), 1-20.

Kline, R. B. (1998). *Principles and Practice of Structural Equation Modeling*: The Guilford Press.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems, 48*(4), 15-24.

Kursan Milaković, I. (2021). Purchase experience during the COVID-19 pandemic and social cognitive theory: The relevance of consumer vulnerability, resilience, and adaptability for purchase satisfaction and repurchase. *International Journal of Consumer Studies, 45*(6), 1425-1442. http://dx.doi.org/10.1111/ijcs.12672

Lee, P. M. (2002). Behavioral Model of Online Purchasers in E-Commerce Environment. *Electronic Commerce Research, 2*, 75-85. http://dx.doi.org/10.1023/A:1013340118965

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(28), 453-496. http://dx.doi.org/10.17705/1CAIS.02828

Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10*(6), 702-715. http://dx.doi.org/10.1016/j.elerap.2011.07.003

Lune, H., & Berg, B. L. (2017). *Qualitative research methods for the social sciences* (9th ed. ed.): Pearson Education.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science, 35*, 572-585. http://dx.doi.org/10.1007/s11747-006-0003-3

Malhotra, N., Kim, 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. http://dx.doi.org/10.1287/isre.1040.0032

Martin-Breen, P., & Anderies, J. M. (2011). *Resilience: A Literature Review*: Bellagio Initiative. IDS.

Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs, 35*(1), 27-44. http://dx.doi.org/10.1111/j.1745-6606.2001.tb00101.x

Oliveira, M. G., & Toaldo, A. M. M. (2015). New times, new strategies: Proposal for an additional dimension to the 4 P's for e-commerce dot-com.com. *Journal of Information Systems and Technology Management, 12*(1), 107-124. http://dx.doi.org/10.4301/S1807-17752015000100006

Pavlou, A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115-143. http://dx.doi.org/10.2307/25148720

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1*(4), 311-335. http://dx.doi.org/10.1111/j.1468-2885.1991.tb00023.x

Popping, R. (2015). Analyzing open-ended questions by means of text analysis procedures. Bulletin of Sociological Methodology. *Bulletin de Methodologie Sociologique, 128*(1), 23-39. http://dx.doi.org/10.1177/0759106315597389

Rajh, E., Škrinjarić, B., & Budak, J. (2021). Otpornost potrošača na narušavanje online privatnosti: Testiranje mjerne ljestvice. *Ekonomska misao i praksa, 30*(2), 527-544. http://dx.doi.org/10.17818/EMIP/2021/2.11

Reed, T. V. (2014). *Digitized Lives: Culture, Power and Social Change in the Internet Era* (1st Edition ed.). New York: Routledge. http://dx.doi.org/10.4324/9780203374672

Rew, D., & Minor, M. (2018). Consumer resilience and consumer attitude towards traumatic events. *Journal of Customer Behaviour, 17*(4), 319-334. http://dx.doi.org/10.1362/147539218X15445233217832

Sharif, M. S., Shao, B., Xiao, F., & Saif, M. K. (2014). The impact of psychological factors on consumers trust in adoption of m-commerce. *International Business Research, 7*(5), 148-155. http://dx.doi.org/10.5539/ibr.v7n5p148

Škrinjarić, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. Economic research. *Economic Research-Ekonomska Istraživanja, 32*(1), 982-1000. http://dx.doi.org/10.1080/1331677X.2019.1585272

Škrinjarić, B., Budak, J., & Žokalj, M. (2018). The effect of personality traits on online privacy concern. *Ekonomski Pregled, 69*(2), 106-130. http://dx.doi.org/10.32910/ep.69.2.2

Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P., & Bernard, J. (2008). The brief resilience scale: Assessing the ability to bounce back. *International Journal of Behavioral Medicine, 15*(3), 194-200. http://dx.doi.org/10.1080/10705500802222972

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). In-formation Privacy: Measuring, Individuals' Concerns about Organisational Practices. *MIS Quarterly, 20*(2), 167-196. http://dx.doi.org/10.2307/249477

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015. http://dx.doi.org/10.2307/41409970

Soopramanien, D. (2011). Conflicting attitudes and skepticism towards online shopping: The role of experience. *International Journal of Consumer Studies, 35*(3), 338-347. http://dx.doi.org/10.1111/j.1470-6431.2010.00945.x

Swinyard, W. R., & Smith, S. M. (2003). Why People (Don't) Shop Online: A Lifestyle Study of the Internet Consumers. *Psychology and Marketing, 20*(7), 567-597. http://dx.doi.org/10.1002/mar.10087

Vears, D. F., & Gillam, L. (2022). Inductive content analysis: A guide for beginning qualitative researchers. *Focus on Health Professional Education: A Multi-Professional Journal, 23*(1), 111–127. http://dx.doi.org/10.11157/fohpe.v23i1.544

Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2008). *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View.* Paper presented at the ICIS 2008 Proceedings, Paris.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. http://dx.doi.org/10.1016/j.dss.2010.11.017

Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model. *Journal of Business Ethics, 100*, 405-417. http://dx.doi.org/10.1007/s10551-010-0687-7

ANNEXES

Table no. A1 – Descriptive statistics of respondents' socio-demographic characteristics

Variable	N	Mean	St. dev.	Min.	Max.
Gender					
Female	513	0.51	0.5	0	1
Male	487	0.49	0.5	0	1
Age[a]	1,000	43.31	15.88	18	86
Age categories					
18-34	347	0.35	0.47	0	1
35-50	304	0.30	0.46	0	1
50+	349	0.35	0.48	0	1
Number of people in household[a]	1,000	3.35	1.42	1	10
Education					
Secondary school or less	538	0.54	0.49	0	1
Higher education	462	0.46	0.49	0	1
Occupation of respondent					
Self-employed	50	0.05	0.22	0	1
Manager	45	0.05	0.21	0	1
Professional	160	0.16	0.37	0	1
Technician/clerk	191	0.19	0.39	0	1
Worker	191	0.19	0.39	0	1
Retired	159	0.16	0.37	0	1
Student	111	0.11	0.31	0	1
Unemployed	93	0.09	0.29	0	1
Income of respondents' household					
Up to 6.500 HRK [b]	182	0.18	0.39	0	1
6.501-10.000 HRK	229	0.23	0.42	0	1
10.001-15.000 HRK	253	0.25	0.43	0	1
> 15.000 HRK	113	0.12	0.32	0	1
No answer	223	0.22	0.42	0	1
NUTS2 region of respondent [c]					
Panonian Croatia	263	0.26	0.44	0	1
Adriatic Croatia	353	0.35	0.48	0	1
City of Zagreb	163	0.16	0.37	0	1
North Croatia	221	0.22	0.42	0	1
Place or residence size					
10,000 or less	309	0.31	0.46	0	1
10,001–50,000	296	0.3	0.46	0	1
50,001–100,000	79	0.08	0.27	0	1
More than 100,000	316	0.32	0.47	0	1

Notes: "St. dev." denotes standard deviation. a As these are not categorical variables, here we present averages rather than frequencies. b 1 EUR ~ 7.5 HRK. c Definitions of these regions are available here: https://ec.europa.eu/eurostat/web/nuts/nuts-maps.

Table no. A2 – Description of items used to build latent constructs

Latent construct	Items	Description
Resilience to online privacy violation (RES)	res_1	I bounced back quickly after the most recent online privacy violation incident.
	res_2	I had a hard time making it through after the most recent online privacy violation incident.
	res_3	It didn't take me long to recover from the most recent online privacy violation incident.
	res_4	It was hard for me to snap back when the most recent online privacy violation happened.
	res_5	I came through the most recent online privacy violation incident with little trouble.
	res_6	It took me a long time to get over the most recent online privacy violation incident.
Online privacy concern (OPC)	opc_1	I am concerned about my online privacy.
	opc_2	I am concerned about extensive collection of my personal information over the Internet.
	opc_3	I am concerned about my privacy violation when using the Internet.
Online privacy awareness (OAW)	oaw_1	I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our online privacy.
	oaw_2	Web sites seeking information about me should disclose the way the data are collected, processed, and used.
	oaw_3	A good online privacy policy should have a clear and conspicuous disclosure.
Internet benefits (BNF)	bnf_1	In general, my need to obtain certain information or services from the Internet is greater than my concern about online privacy.
	bnf_2	The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy online concerns.
Digitalization anxiety (DA)	da_1	Digitalization is a real threat to privacy.
	da_1	I am easily frustrated by increased digitalization in my life.
Protective behavior (PB)	pb_1	I give fictitious responses to avoid giving the web site real information about myself.
	pb_2	I use another name or e-mail address when registering with certain web site without divulging my real identity.
	pb_3	When registering with certain web site, if possible, I only fill up data partially.
	pb_4	I try to eliminate cookies that track my Internet activities.
	pb_5	I try to disguise my identity when browsing (private browsing option).
	pb_6	I refuse to provide personal information to untrustworthy websites.

Table no. A3 – Description of variables in the model

Variable	Description	Values
PV_ser	Privacy violation seriousness scale	1 – Negligibly serious, 2 – Moderately serious, 3 – Medium serious, 4 – Serious, 5 – Very serious
RES	Resilience to online privacy violation	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree
OPC	Online privacy concern	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree
OAW	Online privacy awareness	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree
GIAS	General Internet attitude scale	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree
BNF	Internet benefits	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree

Variable	Description	Values
DA	Digitalization anxiety	1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree
PB	Protective behavior	1 – Never, 2 – Rarely, 3 – Sometimes, 4 – Often, 5 – Very often
Gender	Gender of respondent	1 – Male, 0 – Female
Age	Age category of respondent	1 – 18-34, 2 – 35-50, 3 – 50+
Education	Education of respondent	1 – Secondary school or less, 2 – Higher education (university, college, PhD, MBA, …)
Income	Average household income[a] of respondent	1 – Up to 6.500 HRK, 2 – 6.501-10.000 HRK, 3 – 10.001-15.000 HRK, 4 – More than 15.000 HRK, 5 – Does not want to answer
Region	NUTS 2 region[b] of respondent	1 – Panonian Croatia, 2 – Adriatic Croatia, 3 – City of Zagreb, 4 – North Croatia
Settlement	Settlement size of respondent	1 – 10.000 or less, 2 – 10.001-50.000, 3 – 50.001-100.000, 4 – More than 100.000

Notes: [a] 1 EUR = 7.53 HRK. [b] Definition of NUTS2 regions are available here: https://ec.europa.eu/eurostat/web/nuts/nuts-maps