HOW DATA PRIVACY AFFECTS YOUNG CONSUMERS' TRUST IN ONLINE TRANSACTIONS

Amela JUSUFI[1]

[1*]*Department of Economics, Faculty of Economics and Administrative Sciences, International Balkan University, Skopje, North Macedonia*
[*]*Corresponding author e-mail: amela.jusufi1@ibu.edu.mk*

Abstract

In this study, the focus was on data privacy perceptions and the relation of younger consumers' trust in online transactions. The Technology Acceptance Model, Privacy Calculus model, and an integrated model of online trust were used as a framework for the research. A quantitative cross-sectional approach was chosen as the method, and online survey data were collected from 104 customers aged 18–30 who, in addition to buying online, had at least purchased online one time the 12-month time frame. Four factors are assessed using a five-point Likert scale: perceived privacy threats, privacy policy transparency, data privacy awareness and trust of consumers. Four hypotheses were tested using descriptive methods and correlation measures of Pearson. The relationship between privacy policy transparency ($r=0.548$, $p< .001$) and consumer trust was found quite strong and it was same with data privacy awareness ($r=0.546$, $p<.001$) that it had a significant positive correlation with the trust of consumers. A finding unexpected was that, the perceived privacy risk was not significantly related to overall trust ($r =-0.095$, $p = .338$); but it showed very strongly how privacy related worries affect their inclination to complete a purchase (Privacy risk & reluctance to complete purchases: $r = 0.340$, $p < .001$).The outcome showed that young consumers' trust rested less on the absence of risk than on visible transparency and a sense of informed control, while risk perceptions acted mainly at the moment of transaction. The insights were of practical use for the website sellers, especially to them who had clear privacy information and used trust cues on websites to their customers; and to lawmakers, for whom the awareness of data protection rights is a major factor for building trust.

Keywords: data privacy, consumer trust, online transactions, young consumers, privacy policy transparency, privacy paradox.

1. Introduction

Over the past twenty years, a substantial increase in digital purchasing has largely transformed the entire purchasing, marketing, and data management processes. International retail e-commerce sales have reached 5.8 trillion US dollars and are estimated to reach over 8 trillion by 2027 (Statista 2024). In this context, the consumer's trust will most probably act as a necessary condition for online trading activities: without that trust, people won't freely share personal details, engage in money transactions, or keep digitally interacting (Gefen et al., 2003; McKnight et al., 2002). Trust online is a multi-faceted attribute and comprises not only our reliance on the seller regarding their competence, benevolence and integrity, but also on our belief that the transaction has been conducted through safe and reliable technologies and legal arrangements (Mayer et al., 1995).

At the same time, the occurrence of data breaches, usage of personal data against the person's will, and long, complex privacy policies are all factors that have considerably eroded the confidence of the consumers in the ability of an entity to protect them. Examples of very well-known cases like the Facebook-Cambridge Analytica issue (Confessore, 2018) and huge breaches that happened at several top companies like Equifax, Marriott, and Yahoo have highlighted the inherent flaws of digital data protection to the public. The reactions from the legislative bodies, especially the EU's GDPR, have tried to strengthen individual protection, and put more obligations on data controllers (Voigt & Von dem Bussche, 2017).

Consumers in their late teens up till 30 are central to the discussions regarding privacy and digital economy. As digital natives, they are most probably regular users of Internet-based commerce and mobile payment services (Prensky, 2001). However, they're also said as a group that embodies the 'privacy paradox', expressing deep concern over privacy while not behaving

according to that concern online (Norberg et al., 2007; Acquisti and Grossklags, 2005). The fact that the relationships joining privacy concern, trust, and behavior are not straightforward and are largely situation-bound is reflected in these observations.

This study is driven by numerous points of contention. Many of the initial studies looking at consumer trust of digital transactions were carried out back in the first decade of a new millennium, during time when smartphones and social commerce were still emerging while cloud services had not gained ground (Gefen et al., 2003; Pavlou, 2003). The pathways through which our awareness of the level of privacy a site offers to us results in us trusting them, among others privacy policy transparency and privacy awareness, remain a subject of debate (Dinev and Hart 2006; Smith et al. 2011). Lastly, only a few works have been dedicated solely to the online privacy behavior of customers between 18 and 30 in countries of Southeast Europe, which are rapidly digitizing but, in terms of regulation and infrastructural features, they are quite distinct from that of Western Europe and North America (Eurostat 2023).

The aim is thereby to find out the relationship between consumers' view on data privacy and their trust in making transactions online while at the same time recognizing which factors most significantly influence that trust. Specifically, the study investigates the degree to which consumer trust can be predicted from factors like perceived privacy risk, privacy policy transparency, and data privacy awareness. In addition, it examines whether or not a high level of privacy risk perception is associated with decreased willingness to conduct online transactions. The remainder of the paper reviews the literature and develops the hypotheses, describes the methodology, presents and discusses the results, and closes with conclusions and limitations.

2. Literature Review

2.1 Consumer trust in online transactions: Trust means one party's vulnerability to another's behavior, trusting based on the expectation that the second party would do something significant to the trustor, even if the trustor couldn't monitor or control that party (Mayer et al., 1995). According to Gefen et al. (2003), trust can be divided into two types in e-commerce, the vendor's trust, which is the online seller's trust, and Internet's trust, a medium of exchange. Also, Pavlou (2003) showed that trust helps people overcome uncertainty and enables them to conduct shopping activities. Trust keeps changing it develops gradually through an experience in which one gets to know the other and relies on them after that, besides the experience, one trusts the person based on the sign, like third-party certifications, a well-explained privacy policy and a quick response to the customer (Bart et al., 2005; Kim et al., 2008). Antecedents of trust identified in the literature are website quality and usability, familiarity with the vendor (Gefen, 2000), social presence (Hassanein and Head, 2007) as well as the availability of privacy and security policies (Milne and Culnan, 2004). In the case of lack of trust, customers may not only abandon transactions and leave platforms but also engage in self-protective behaviors such as cookie refusal or giving incorrect information (Dinev & Hart, 2006; Awad & Krishnan, 2006).

2.2 Theoretical background: Four frameworks have been used to underpin this study. The Technology Acceptance Model (Davis, 1989) describes technological adoption in terms of perceived usefulness and ease of use. In the case of e-commerce, the model was augmented by trust and perceived risk. Pavlou (2003) demonstrated that the more a person perceiving risk the less their intention to transact, but on the contrary, trust may mitigate the risk. Privacy Calculus Theory (Dinev and Hart, 2006) states that people calculate the perceived price for information disclosure vs. the perceived gains (e.g. convenience, personalization). Furthermore, trust is a factor that makes people more sure that they will get the rewards over the costs of disclosing.

It was later found out that privacy calculus was also limited by emotions, social norms, and cognitive biases (Acquisti et al., 2015) which influence individual's rational decision making. McKnight et al. (2002) differentiated between the three elements of trust (the ability, the goodwill, and the honesty), as well as institutional-based structural guarantees like legal protection and industry standards which is very important as regulation of privacy and its enforcement are at a very dynamic stage. The last theory is the Theory of Planned Behavior (Ajzen, 1991) that gives a reason as to why privacy concerns do not always lead to protecting behavior when sharing data is socially acceptable (Youn, 2009).

2.3 Perceived privacy risk: Information privacy refers to individuals' capability to decide when and to what extent their personal data is gathered, employed and revealed (Westin, 1967; Smith et al., 2011). According to this definition, perceived privacy risk is an individual's estimation of how probable negative consequences such as illegal access, identity takeover, or unwanted marketing or the selling of data to third parties are (Featherman and Pavlou, 2003). Besides, Malhotra et al. (2004) who introduced the Internet Users' Information Privacy Concerns (IUIPC) scale identified that people's concern about privacy was an important factor negatively associated with their beliefs of trust and their intention to engage in an activity. Also, Featherman and Pavlou (2003) concluded that privacy risk can diminish an individual's willingness to adopt electronic services, even when the other risk factors are taken away from the analysis. These feelings are also exacerbated by breaches: Janakiraman et al. (2018) revealed that disclosing the breach could affect customers' purchasing behavior in the affected shops. All these findings make us state the hypotheses H1 and H4 of the research.

2.4 Privacy policy transparency: Privacy policies are the main way that companies reveal their data handling practices to users, yet they tend to be long, legalistic, and rarely read. McDonald and Cranor (2008) estimated that if one reads all the privacy policies encountered in a year, it will take them 76 working days. Milne and Culnan (2004), however, found that a privacy notice, even if its content was barely read, was connected with a high level of trust, so that transparency can also be regarded as a form of a visible act of a company. The use of simplified standardized format such as privacy "nutrition labels" has been proved effective in terms of comprehension and evaluation of organizations (Kelley et al., 2009). Bart et al. (2005) showed that privacy and security were the prime determinants of trust on sites with a high level of risk such as financial services. This supporting set of facts leads to Hypothesis H2.

2.5 Data privacy awareness and the regulatory context: The GDPR gives people the right to access their data, rectify incorrect data, delete the data, port the data to another service and object to it's processing and it requires organizations to have a lawful basis, minimize data and inform the users in plain language (Voigt and Von dem Bussche, 2017). Regulations can also enhance the structural-assurance dimension of trust via lowering information asymmetry and establishing supervisory authorities with the enforcement powers (Martin and Murphy, 2017). However, the effectiveness of the regulation greatly depends on consumer's familiarity with their rights, which is yet to be equal (Eurobarometer, 2020), and Degeling et al. (2019) demonstrated that the majority of website designers kept on using manipulative consent features long after GDPR was in full effect. Therefore, how strongly perceived risk turns into distrust may depend on awareness and this is why our hypothesis H3 is based on such line of reasoning.

2.6 Young consumers and the privacy paradox: Millennials and Generation Z, who constitute the majority of the 18-30 demographic, are the most frequent users of e-commerce, social media and digital payments. However, the idea of a uniformly digitally skilled generation as

"digital natives" has been criticized as an overgeneralization (Bennett et al., 2008). Youth expressed a considerable amount of interest in how their personal data was used through different means (Pew Research Center, 2019), though most of them still choose to voluntarily share the data in order to receive slight benefits or rewards (Acquisti and Grossklags, 2005; Norberg et al., 2007). It is argued that this discrepancy can be due to optimism bias, present bias, acceptance of default settings (Acquisti et al., 2015), and also to a sense of control (Brandimarte et al., 2013). Kokolakis (2017) found that the level of the paradox depends on the sensitivity of the information, how trustworthy the one who is going to get the information is perceived to be and how prominent the risk aspect is at the moment of making the decision and this indicates that it should be a research focus in specific transactional situations.
Based on the review literature, the following hypotheses were formulated:

- **H1:** Perceived privacy risk is negatively associated with young consumers' trust in online transactions.
- **H2:** Greater privacy policy transparency is positively associated with young consumers' trust in online platforms.
- **H3:** Data privacy awareness moderates the relationship between perceived privacy risk and consumer trust.
- **H4:** Higher perceived privacy risk is associated with lower willingness of young consumers to complete online transactions.

3. Methodology

3.1 Research design and sample: The study was based on the deductive, quantitative approach and used a descriptive cross-sectional survey, a design suitable for measuring attitudes, perceptions, behavioral intentions, and the relationships among them (Bryman,2016; Saunders et al.,2019). The primary sample included people with e-transaction experience such as e-commerce purchase, digital payment or online banking aged 18-30. Limited time and access led to using the convenience sampling, the survey was delivered online and via social media, mostly on the campuses. Only the respondents aged 18–30 and who had performed one online transaction at least during the past 12 months were taken into the final dataset with a sample size of 104. Participation in this study was not a requirement but was entirely voluntary, anonymous data collection, and the data were used solely for academic purposes.

3.2 Instrument: Data was collected via a standardized, self-completed questionnaire that the participants filled in Google Forms. The whole questionnaire lasted for about five to seven minutes. Demographic data were collected in Section A such as age, sex, level of education, how often they go online for transactions, main device type and past experiences of data breaches. The other sections used four different measures with items borrowed from existing and reliable scales: perceived privacy risk (PPR; 4 items; Featherman and Pavlou, 2003; Malhotra et al., 2004), privacy policy transparency (PPT; 4 items; Milne and Culnan, 2004; Bart et al., 2005), data privacy awareness (DPA; 4 items; Smith et al., 2011; Eurobarometer, 2020.) and consumer trust (CT; 5 items; McKnight et al., 2002; Gefen et al., 2003). Participants were to score everything on a five-point Likert scale. (1 = strongly disagree, 5 = strongly agree).

3.3 Data Analysis: Demographic variables are presented by frequencies and percentages. Items were first individually analyzed as mean, standard deviation, and share of "agree" and "strongly agree" responses and aggregated into composite construct scores by taking a mean of the items (Malhotra et al., 2004). Item Q21 "My concerns about data privacy reduce my willingness to complete purchases on online platforms" was a negatively worded sentence which has been reverse-scored before obtaining the consumer trust composite. Pearsons's correlation

coefficients then indicate the direction and strength of the hypothesized relationships between the four composite scores.

4. Results

4.1 Sample profile: Respondents who were aged from 18 to 23 (77.9%) dominated the sample alongside women participants (60.6%) and students who were taking bachelor studies (78.8%) which clearly indicates the characteristics of the university-based and convenient sample (Table 1). Online transactions were quite active with 55.7% of the respondents stating they at least several times a week. For 73.1%, their smartphone was mainly used as a transaction device, 16.3% had themselves experienced a cybercrime, or their data had been compromised, while 26.9% of participants were not quite sure.

Table 1. Demographic profile of respondents (N=104)

Variable	**Category**	**n**	**%**
Age	18-20 years	40	38.5
	21-23 years	41	39.4
	24-26 years	11	10.6
	27-30 years	12	11.5
Gender	Female	63	60.6
	Male	41	39.4
Education	Secondary school	5	4.8
	Bachelor’s degree (in progress)	82	78.8
	Bachelor’s degree (completed)	9	8.7
	Master’s degree or higher	8	7.7
Frequency of online transactions	Daily	28	26.9
	Several times a week	30	28.8
	Several times a month	30	28.8
	Less than once a month	16	15.4
Primary Device	Smartphone	76	73.1
	Multiple devices equally	19	18.3
	Laptop or desktop	8	7.7
	Tablet	1	1.0
Data breach experience	Yes	17	16.3
	No	59	56.7
	Not sure	28	26.9

4.2 Descriptive statistics: The means of all four constructs were near the scale midpoint (Table 2). Perceived privacy risk (M=3.29, SD=0.89) expressed a moderate level of concern, privacy policy transparency (M=3.35, SD=0.80) showed a slight tendency to regard platforms as transparent, while data privacy awareness (M=3.34, SD=0.74) demonstrated a moderate to high level of self-assessed knowledge about privacy rules and practices. Consumer trust was at the lowest level (M=3.20) and had the smallest variance (SD=0.57), this means that consumer 's trust was moderate and their responses were clustered around the median.

Table 2. Descriptive statistics for the main constructs (N=104)

Construct	Items	Mean	SD	Min	Max
Perceived privacy risk (PPR)	4	3.29	0.89	1.00	5.00
Privacy policy transparency (PPT)	4	3.35	0.80	1.00	5.00
Data privacy awareness (DPA)	4	3.34	0.74	1.00	5.00
Consumer trust (CT)	5	3.20	0.57	1.60	4.60

4.3 Item-level results: Neutral responses were the most frequent answer on most items, ranging from around 42 to 45% on the risk-related questions and going up to almost 50% on two trust-related questions (Q22 and Q23). However, within each domain, a clear difference was observed (Table 3). Among the risk items, agreement was highest on the question about fear of financial fraud when entering payment details (Q9, agreement 39.4%) was the biggest concern. Q13 was the highest-rated item overall: 56.7% of respondents agreed that having a visible and clear privacy policy made one more confident to make a transaction (M = 3.77). On the contrary, only 30.7% of people believed that most platforms are really transparent as to why they collect data (Q14, M = 3.10). Respondents were more confident about knowing and understanding their rights (Q18, M = 3.46) than they were about what data specific platforms collect (Q16, M = 3.15) within awareness. Trust: confidence in completing transactions on familiar platforms (Q20, M = 3.55) was clearly higher than trust in vendors' handling of personal information (Q19, M = 3.18).

Table 3. Item-level descriptive statistics

Item	Statement (abbreviated)	Mean	SD	% Agree
Q7	Risk of unauthorized access to personal information	3.30	1.10	36.5
Q8	Vendors may share or sell data to third parties	3.27	1.11	35.6
Q9	Payment information exposes me to financial fraud	3.32	1.05	39.4
Q10	Data may be used for purposes I did not agree to	3.28	1.13	35.6
Q11	Platforms clearly explain how they collect and use data	3.27	1.09	36.5
Q12	Privacy policies are easy to understand	3.26	1.22	39.4
Q13	A visible, clear privacy policy increases my confidence	3.77	1.11	56.7
Q14	Most platforms are transparent about data collection purposes	3.10	1.08	30.7
Q15	Awareness of GDPR and similar regulations	3.34	0.97	37.5
Q16	Knowledge of the types of data platforms collect	3.15	1.03	33.7
Q17	I actively take steps to protect my personal data	3.39	1.08	43.3
Q18	I understand my rights regarding my personal data	3.46	0.96	42.3
Q19	Vendors will handle my personal information responsibly	3.18	1.00	31.7
Q20	Confidence completing transactions on familiar platforms	3.55	1.05	50.0
Q21 (R)	Privacy concerns reduce my willingness to purchase	3.27	1.08	37.5
Q22	Platforms have sufficient security measures	3.26	0.97	34.6
Q23	The legal framework adequately protects my data	3.26	0.98	33.7

Note: Q7-Q10 = PPR; Q11-Q14 = PPT; Q15-Q18 = DPA; Q19-Q23 = CT. % Agree = share of "agree" and "strongly agree". (R) = reverse-coded in the CT composite; values shown are raw responses.

4.4 Relationships between constructs: Pearson correlation coefficients are displayed in Table 4. Privacy policy transparency (r=0.548, p< .001) and the level of consumer data privacy awareness (r=0.546, p< .001) were strongly and positively correlated to consumer trust. In contrast, the relationship between perceived privacy risk and consumer trust was minimal (r= -0.095, p= .338) and non-significant. Transparency and awareness were also strongly connected with each other (r=0.680, p< .001). Moreover, although, in comparison, very small, the link between perceived privacy risk and awareness was found to be statistically significant (r=0.206, p< .05).

Table 4. Pearson correlation matrix of the composite constructs (N=104)

	PPR	**PPT**	**DPA**	**CT**
PPR	1.000			
PPT	0.134	1.000		
DPA	0.206*	0.680**	1.000	
CT	-0.095	0.548**	0.546**	1.000

*Note: * p < .05; ** p < .001.*

4.5 Hypothesis testing: Table 5 depicts the summary of the findings. H1 was not confirmed while H2 was. H3 hypothesis cannot be tested as a moderation hypothesis first, because the correlational analysis did not include an interaction term, and even the PPR-CT relationship was not significant. However, awareness was directly and closely related to trust. For H4, item Q21 reflects willingness to transact. Even though perceived privacy risk was not associated with the trust composite, the two variables still had a significant and positive correlation with agreement that privacy concerns would reduce willingness to purchase (r = 0.340, p <.001). That is, individuals who perceived their privacy risk as higher would be more likely to say they were reluctant to take the action; thus, the H4 was corroborated.

Table 5. Summary of hypothesis testing

Hyp.	**Statement**	**Result**	**Evidence**
H1	PPR is negatively associated with CT	Not supported	r = -0.095, p= .338
H2	PPT is positively associated with CT	Supported	r = 0.548, p < .001
H3	DPA moderates the PPR-CT relationship	Not tested as moderation	DPA-CT r =0.546, p < .001 (direct association)
H4	Higher PPR is associated with lower willingness to transact	Supported	PPR – Q21 r = 0.340, p < .001

5. Discussion

5.1 Privacy risk and trust: The fact that a strong relationship between perceived privacy risk and trust is no longer found in a study as opposed to a study earlier which showed that link (Malhotra et al., 2004) is somewhat perplexing though it is very much in line with the Privacy paradox (Norberg et al., 2007; Kokolakis, 2017). It is quite logical to suppose, after such findings, that young adults have come to treat a low level of privacy risk as something quite normal and therefore unavoidable for anyone using the Internet. As a result, perceptions of risk no longer affect trust in general. When viewed from the Privacy Calculus theory (Dinev and Hart, 2006) it is quite evident that for young adults' convenience, speed and the social perks of

doing business online would most likely outweigh the costs of privacy loss. Besides, the fact that PPR and trust responses are closely centered around a neutral point gives us the idea that ambivalence rather than definite attitudes is what explains the relationship of young people to privacy risk.

5.2 Transparency as a trust signal: Privacy policy transparency was one of the two strongest correlates of trust which shows how visible privacy policies can be a signal of accountability even when the content is not read in detail (Milne and Culnan, 2004). The differences between the answers to Q13 and Q14 are particularly revealing: the respondents rated transparency very high but at the same time they did not believe most platforms offered it. The discrepancy in the expectation for and reality of transparency is supported by the fact that formal GDPR compliance does not always equate to real transparency (Degeling et al., 2019) and it shows that platforms will be trusted if they give clear, simple privacy communications rather than only through objective risk reduction.

5.3 Awareness as empowerment: Bigger knowledge of privacy could be thought of as making consumers more critical. On the contrary, being aware of such aspects is largely and favorably correlated with trust. We can understand this as being in tune with the concept of a structural assurance that is part of the model by McKnight et al. (2002): If an individual is familiar with the GDPR provisions and also makes efforts to safeguard their data they may feel more capable and thus more inclined to trust. After all, one's belief in their ability to control things is a factor that affects the decision of disclosure (Brandimarte et al., 2013; Acquisti et al., 2015) and therefore that link needs to be carefully considered. Moreover, the strong relationship between awareness and transparency points to the fact that privacy-conscious consumers are more likely to respond to transparency cues, thereby reinforcing the positive connection of the two constructs with trust.

5.4 Risk at the moment of transaction: Risk perception was found to be only marginally linked with the level of general trust, but they were linked with consumers' reluctance in a buying context. This confirms Pavlou's (2003) result that risks can deter transaction intention and points, theoretically, to a useful distinction: trusting is a reasonably stable attitude while a readiness to make a transaction is a contextual intention which is sensitive to risk cues at the moment of decision. The checkout, where buyers are required to reveal both financial and personal details and where 39.4% experienced the fear of financial fraud has therefore emerged as an individual point of friction where conversion could be impacted even by consumers who have an overall positive opinion of the website.

5.5 Overall reflection: The results when taken as a whole imply that the young generation's confidence in online shopping has more to do with the presence of positive signals such as open communication, visible responsibility and understanding of one's rights than just with the absence of risk. It explains privacy paradox more thoroughly as in this group trust may just be shifting in favor of being transparent and being empowered rather than people just being irrational or ignorant.

6. Conclusions

In this study, the links between perceived data privacy and trust levels in online transactions were investigated among a group of 104 consumers aged 18-30. Trust was most positively related to privacy policy transparency and data privacy awareness while perception of privacy risk had little impact on the overall trust but was connected with lesser willingness to buy. The

results indicate that simply lowering perceived risk cannot be the sole factor that contributes to building trust among young consumers. Rather, trust can be grounded in transparency and privacy empowerment. Theoretically, they confirm the ongoing importance of structural assurances (McKnight et al., 2002), the role of privacy policy for communication and information (Milne & Culnan, 2004), and they differentiate between the privacy-attitudinal impact on trust from and the behavioral impact in the moment of a transaction.

Many of the results can be implemented immediately. For online vendors, the study advises that they use the design of communicating privacy issues through easy-to-understand, short-language versions of the privacy policies as well as layering disclosures and privacy dashboards that empower users with control over and understanding of their settings. The trust markers at the time of payment, namely security icons, small data use clarifications and a mechanism which clearly states that the consumer consents to the data collection should be displayed, where the risk perceptions of the consumer will be most intense. Companies may also assist consumer privacy education through clear onboarding and easily accessible information on users' rights. As to the policymakers, the association between a consumer being aware of his data protection rights and his trust indicates that digital literacy initiatives, campaigns explaining consumers rights under the data protection regulations can benefit not only consumers but also foster the growth of the digital economy.

Limitations of the study are worth pointing out. The sample of the people that was used was quite convenient. University students comprised most of the participants and it is, therefore, difficult to generalize the results to all consumers aged 18–30. It is impossible to determine causality with the cross-sectional nature of the study and the data collection method, it was not able to formally investigate the moderating role of awareness, and lastly, because the survey was self-administered the results might have suffered from an unconscious desire to please (social desirability bias). Future studies should incorporate probability sampling methods, longitudinal and multivariate techniques such as regression and structural equation modelling including formal moderation testing. By way of transaction types (e.g. social networking vs. banking) and different regulatory regimes, as far as the emotional and cognitive side of privacy decisions is concerned, qualitative research could further enrich these results.

Nomenclature

CT	Consumer Trust
DPA	Data privacy awareness
GDPR	General Data Protection Regulation
PPR	Perceived privacy risk
PPT	Privacy policy transparency

References

[1]. Acquisti A. and Grossklags J., 2005. Privacy and rationality in individual decision making. IEEE Security & Privacy, Vol. 3, No. 1, pp. 26-33.

[2]. Acquisti A., Brandimarte L. and Loewenstein G., 2015. Privacy and human behavior in the age of information. Science, Vol. 347, No. 6221, pp. 509-514.

[3]. Ajzen I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes, Vol. 50, No. 2, pp. 179-211.

[4]. Awad N.F. and 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, Vol. 30, No. 1, pp. 13-28.

[5]. Bart Y., Shankar V., Sultan F. and Urban G.L., 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, Vol. 69, No. 4, pp. 133-152.

[6]. Bennett S., Maton K. and Kervin L., 2008. The 'digital natives' debate: A critical review of the evidence. British Journal of Educational Technology, Vol. 39, No. 5, pp. 775-786.
[7]. Brandimarte L., Acquisti A. and Loewenstein G., 2013. Misplaced confidences: Privacy and the control paradox. Social Psychological and Personality Science, Vol. 4, No. 3, pp. 340-347.
[8]. Bryman A., 2016. Social research methods. 5th ed. Oxford University Press, Oxford.
[9]. Confessore N., 2018. Cambridge Analytica and Facebook: The scandal and the fallout so far. The New York Times, 4 April 2018.
[10]. Davis F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, Vol. 13, No. 3, pp. 319-340.
[11]. Degeling M., Utz C., Lentzsch C., Hosseini H., Schaub F. and Holz T., 2019. We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy. Proceedings of the Network and Distributed System Security Symposium (NDSS 2019), San Diego.
[12]. Dinev T. and Hart P., 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research, Vol. 17, No. 1, pp. 61-80.
[13]. Eurobarometer, 2020. Data protection in the EU: Europeans' attitudes towards data protection and digital technologies. European Commission, Brussels.
[14]. Eurostat, 2023. E-commerce statistics for individuals. Eurostat Statistics Explained, Luxembourg.
[15]. Featherman M.S. and Pavlou P.A., 2003. Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, Vol. 59, No. 4, pp. 451-474.
[16]. Gefen D., 2000. E-commerce: The role of familiarity and trust. Omega, Vol. 28, No. 6, pp. 725-737.
[17]. Gefen D., Karahanna E. and Straub D.W., 2003. Trust and TAM in online shopping: An integrated model. MIS Quarterly, Vol. 27, No. 1, pp. 51-90.
[18]. Hassanein K. and Head M., 2007. Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. International Journal of Human-Computer Studies, Vol. 65, No. 8, pp. 689-708.
[19]. Janakiraman R., Lim J.H. and Rishika R., 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. Journal of Marketing, Vol. 82, No. 2, pp. 85-105.
[20]. Kelley P.G., Bresee J., Cranor L.F. and Reeder R.W., 2009. A "nutrition label" for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09), Mountain View.
[21]. Kim D.J., Ferrin D.L. and Rao H.R., 2008. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, Vol. 44, No. 2, pp. 544-564.
[22]. Kokolakis S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, Vol. 64, pp. 122-134.
[23]. Malhotra N.K., Kim S.S. and Agarwal J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, Vol. 15, No. 4, pp. 336-355.
[24]. Martin K.D. and Murphy P.E., 2017. The role of data privacy in marketing. Journal of the Academy of Marketing Science, Vol. 45, No. 2, pp. 135-155.
[25]. Mayer R.C., Davis J.H. and Schoorman F.D., 1995. An integrative model of organizational trust. Academy of Management Review, Vol. 20, No. 3, pp. 709-734.
[26]. McDonald A.M. and Cranor L.F., 2008. The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, Vol. 4, No. 3, pp. 543-568.
[27]. McKnight D.H., Choudhury V. and Kacmar C., 2002. Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, Vol. 13, No. 3, pp. 334-359.
[28]. Milne G.R. and Culnan M.J., 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, Vol. 18, No. 3, pp. 15-29.
[29]. Norberg P.A., Horne D.R. and Horne D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, Vol. 41, No. 1, pp. 100-126.
[30]. Pavlou P.A., 2003. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, Vol. 7, No. 3, pp. 101-134.
[31]. Pew Research Center, 2019. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Pew Research Center, Washington D.C.
[32]. Prensky M., 2001. Digital natives, digital immigrants. On the Horizon, Vol. 9, No. 5, pp. 1-6.
[33]. Saunders M., Lewis P. and Thornhill A., 2019. Research methods for business students. 8th ed. Pearson, Harlow.
[34]. Smith H.J., Dinev T. and Xu H., 2011. Information privacy research: An interdisciplinary review. MIS Quarterly, Vol. 35, No. 4, pp. 989-1015.
[35]. Statista, 2024. Retail e-commerce revenue worldwide from 2019 to 2027. Statista, Hamburg.
[36]. Voigt P. and Von dem Bussche A., 2017. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, Cham.

[37]. Westin A.F., 1967. Privacy and freedom. Atheneum, New York.
[38]. Youn S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs, Vol. 43, No. 3, pp. 389-418.