The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach

M Dimodugno¹,*, S Hallman², M Plaisent³ and P Bernard¹
¹Department of CIS, Smith Technology Center, Bentley University Waltham MA 02452 USA
²Department of Info Tech School CIS University of the Cumberlands, Williamsburg, KY 40769 USA
³Department of Management, University of Quebec at Montreal, Montreal, H3C3P8, Canada

*Corresponding author: e-mail: mdimodugno@bentley.edu

Abstract: The rapid developments and innovations in technology have created unlimited opportunities for private and public organizations to collect, store and analyze the large and complex information about users and their online activities. Data mining, data publishing, and sharing sensitive data with third parties help organizations improve the quality of their products and services and raise significant individuals' privacy concerns. Privacy of personal information remains subject to considerable controversy. The problem is that big data analytics methods allow user's data to be unlawfully generated, stored, and processed by leaving users with little to no control over their personal information. This quantitative correlational study measures the effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information in the context of big data analysis. The key research question aimed to examine the relationship among the variables of perceived privacy concerns, perceived privacy risk, perceived privacy control, and trust. Drawing on Game Theory, the study explores all the game players' actions, strategies, and payoffs. Correlation analysis was used to test these variables based on the research model with 418 internet users of e-services in the United States. The overall correlation analysis showed that the variables were significantly related. Recommendations for future studies are to explore e-commerce, e-government, and social networking separately, and data should be collected in different regions where many factors can affect the privacy concerns of the individuals.

1. Introduction to the Study

Technological developments for service delivery and social media empower people to access, retrieve and use the information to fulfill their needs. These developments influence and transform lives every day; the way people work, the consumption of goods and services, communication, and interaction. Advances in information technology have also brought privacy concerns as private and government organizations store, process, and exploit personal data using big data analytics. Personal information in digital format can be easily copied, transmitted, and integrated, enabling online marketers to construct thorough individuals' descriptions and profiles [1, 2, 3, 4]. Unauthorized access, secondary use, and the interception and misuse
of personal information are the main factors creating privacy concerns for online users. The two main antecedents of these privacy concerns are perceived privacy risk and perceived privacy loss, becoming a roadblock for gaining customer's consent [5]. Privacy concerns and trust significantly affect individual perceptions of information practices [6]. Using a quantitative survey research design, this study examines the effect of privacy concerns, risk, control, and trust in individual's decisions to share data with organizations.

1.1 Background of the Study

Big data is intensively integrated into every aspect of people's lives and in every industry, including telecommunication, healthcare, business, finance, academia, energy, and government entities [7]. Big data creates capabilities to search, aggregate, and cross-reference large data sets [8]. Private and government organizations develop new growth opportunities by analyzing data collected and making it part of their decision-making process. These tremendous opportunities also introduce privacy and security issues to the individuals providing the data. Personal information security issues are becoming increasingly severe, including the breach of personal information, the potential security risks, and the users' reduced personal information control rights [9].

As the concerns for protecting personal information during big data analysis grow, organizations look for ways to create or improve privacy assurance mechanisms, which give them the ability to build consumers' trust and comply with the laws and regulations [10]. Context matters in designing privacy assurance mechanisms because what works for e-commerce or social media doesn't work for government organizations where provisioning data is mandatory by law [11]. Government organizations handle more sensitive data than any other sector. These agencies are the biggest target of malicious activities, given the amount of sensitive information collected and stored like social security numbers, birth date, birthplace, addresses, and other personal information. Surveillance is a crucial part of government service, where sensitive data is collected, stored, and analyzed for various purposes; sometimes, those purposes are not disclosed to the citizens [12]. The e-commerce space is different, where it is argued that individuals make their own decisions to share personal and financial information engaging in transactions with various companies. Personal information is vital for e-commerce companies because it allows them to use big data analysis and uncover customers' shopping behavior [13, 14, 15].

With the proliferation of big data, pre-existing privacy data management policies and controls such as consent, transparency, individual's right to access the data, the purpose of collection and use of the data need to change and address the privacy concerns and protect individuals from data breaches. Financial data leakage or any violation of privacy can have multifold losses for customers, and sometimes the damage can be irreversible [16]. The privacy principles that organizations had set before might not work now that big data introduces other ways of analyzing the information. These principles should reflect the definitions of privacy and its protection at the core [17].

1.2 Problem Statement

Big data analytics has become a great asset for organizations to extract valuable insights from user's data. The increasing access and process of sensitive information can directly jeopardize an individual's privacy [18, 19; 20, 21]. The techniques used in business analytics recently can reveal more than consumers can ever imagine. An example of that is the sensitive information of an Online Social Network OSN user, who can be discovered through advanced data mining techniques, even if the individual does not directly disclose the information. Data miners with malicious intent can build a decision tree or forest from a data source with information about many OSN users. Based on that information, data miners can learn general patterns [22]. The problem this study examines is that big data analytics methods allow user's data to be
unlawfully generated, stored, and processed, leaving with little to no control over their personal information [23, 24, 25, 26, 27].

1.3 Purpose of Study
The purpose of this quantitative correlational study is to measure the effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information in the context of big data analysis. These variables can significantly affect an individual's decisions, whether to disclose personal information or not. The online shopping environment, for instance, has specific characteristics, which result in specific perceived risks by the consumers with different characteristics from the offline context [28]. The perception of risk is a significant obstacle to the growth of e-commerce and the competitive advantage for organizations. Having control over the data is essential, and it changes the decisions people make and the behavior expressed in disclosing personal information. New technological developments have introduced new challenges regarding personal data protection due to the large amount of personal information published and shared [29]. Understanding to what extent individuals want to exert control over their data disclosure is critical in protecting privacy [30]. If the individual’s perceived risks are higher than the benefits of sharing the information or if the individual perceives a lack of control over the data, privacy concerns start to surface and impact the decisions of sharing personal information. Adding to these concerns, the trust factor, where the individual does not trust the privacy assurance mechanisms the organizations have created, makes it harder for the individual to disclose personal information [31].

Consumers' overall experience with a specific organization is based on their affective evaluations. Individuals' perception of trust can be influenced by these affective evaluations based on many things, including but not limited to the firm's reputation or personal experience with the organization [32]. Organizations can enhance individuals' trust through their privacy assurance mechanisms. Privacy policy statements and privacy assurance mechanisms provide cues to the consumers. Those cues are among the essential website features that an online provider can use to increase individuals' trust and willingness to disclose private information online [33]. The organizations' responsibility is to ensure that when the consumer has shared personal information with them, information will be stored and used for disclosed purposes and will not be shared with their parties without consent and agreement from the individual.

1.4 Significance of the Study
This research study navigates through important privacy issues experienced by consumers using e-services. Decisions that individuals make are based on critical aspects, including weighing risks versus benefits, the control they perceive to have over their data, and the trust factor. The potential significance of this research study in the body of knowledge is the examination of privacy issues and concerns through the lens of an individual's perceptions of risk, control, and self-disclosure behavior impacted by the trust factor. The study aims to explain how decisions are made by the individual and what affects these decisions while sharing personal information with organizations from data mining techniques used in big data analytics. The model used for this study, which was tested and validated before this research by [5], in combination with the Game Theory, will add value by exploring the correlations among variables and constructs. Unique value-added is also the effect of age, gender, and level of education in perceived privacy concerns, perceived privacy risk, perceived control, and trust, which is also part of this study.

2 Theoretical Framework
The effect that organizational privacy assurances have on individual perceptions, privacy concerns, risk, control, trust, and information disclosure has been explored by [5]. The model has seven constructs: perceptions of the privacy policy, perceptions of organizational privacy self-regulation, two mediating variables: privacy risk and control perceptions, and three dependent variables: privacy concerns, trust,
non-self-disclosure behavior. The research model examines how individual risk-control perceptions may influence privacy concerns, trust, and non-self-disclosure behavior and the direct effect of organizational privacy assurance mechanisms on individual perceptions and consequences, privacy concerns, trust, and non-self-disclosure behavior. Through these relations, the model also provides a way to check if the effect of organizational privacy assurances on perceived privacy concerns, trust, and self-disclosure behavior can be mediated by control and risk perceptions [5]. In this research, the model is applied to show how these constructs influence the individual's decision-making process in sharing information. In addition to that, this model is placed in the context of business analytics using data mining techniques to show unlawful access and use of individuals' data.

2.1 Research Model

Illustration of the research model [5]. Reprinted with permission.

The theoretical framework for this research study is based on Game Theory. This theory analyzes situations in which parties called players make interdependent decisions against incentives. The interdependence causes each player to consider other players' possible decisions and strategies to formulate their own decisions. The optimal decision of the players is the solution for the game. The players could have similar, opposed, or diverse interests, which will derive the outcomes from their decision-making process. The essence of Game Theory is strategic thinking, which is critical for this research and the decisions made by individuals and organizations to receive an incentive or maximize their profits. This theory helps convey the understanding of the relationships made and broken during engagement in competition. The theory of independent and interdependent decisions and the strategic foundation for a given situation at a given time is the central tenant of Game Theory.

Gaming Theory's application is as old as life itself, and the theory is applied daily to people's lives and the decisions made under certain conditions. The formal literature can be traced back to [34], who created the zero-sum games. The paper by [35] marked a significant advancement in the Game Theory by creating the Nash Equilibrium that would be the base for many research studies in economics, politics, and computer science. Each player has a strategy in the game. The player chooses specific actions based on what the player has seen happen so far in the game. Suppose none of the players can increase the expected payoff by changing their strategy while the other players keep their strategy unchanged. In that case, the current set of strategy choices constitutes a Nash equilibrium [35]. The Nash equilibrium concept offers a
unique framework for understanding the users' strategic behavior and their decisions to share their information with various companies. On the other hand, the companies apply their strategic decisions in the process, and their goal is to maximize their payoffs. To do so, companies respond strategically to the consumers' privacy concerns.

Game theory is a role-based framework with the players, actions, strategies, and payoffs. The theory in this research study is put in the context of data mining or knowledge discovery that takes place when the users provide information to private or government organizations. The information is collected and used to derive specific results, which will serve as valuable insights for the companies. Sometimes companies also make decisions on sharing the information with third parties. Data providers, data collectors, data miners, and decision-makers are the main players in the game. Each of them has their strategy and actions, and based on their strategies; they get the payoffs [36]. The game in this study is a dynamic one because decisions are not made simultaneously. In a dynamic game, players move sequentially; all the players know the game rules and maximize their payoffs, knowing the other players are doing the same. The game is an extended form in the data mining process because of the players' sequential movement. The players find Nash Equilibrium when they don't deviate from their strategy, given that the other players don't deviate either. If they deviate from the strategy, the payoff is 0, which is not profitable.

2.2 Research Paradigm
This study analyzes the relationship between the independent variables age, gender, and level of education and the dependent variables privacy concerns, risks, control, and trust of professional workers in social networks. The study uses a quantitative correlational research design. During the planning stage of the research design, this study considered two primary methodologies, namely qualitative and quantitative research methods, widely used in research studies. Quantitative methods are designed to deal with numbers and anything measurable in a systematic way of investigating phenomena and their relationships. This method answers the questions on relationships within measurable variables to explain, predict, and control a phenomenon [37].

This research followed a quantitative research paradigm, including methodology and survey instrument. Survey results are statistically analyzed in this study. The survey's history can be traced back to the ancient time census, which involves collecting data from the entire population in a particular geographical entity. Recently, with the achievements of information technology, surveys continue to transform and enhance data collection's ability [38]. The survey instrument for this study was created by [5], and the authors obtained permission to use the survey. The survey was used to study the individuals' behavior in e-services and the effect of organizational privacy assurance on that behavior. Model development considers the aspects of privacy, risk, trust, information disclosure, and organization's privacy policies, standards, and controls. This study is based on an individual's decisions to disclose personal information and decisions that the organizations need to make to provide privacy assurance mechanisms effective enough to protect individual's personal information. Therefore, a quantitative study was appropriate in discovering how these decisions are made based on the methodology and theoretical approach.

2.3 Research Design
Research design serves as the framework used to plan, implement, and analyze the study. The proper choice of a suitable research methodology can provide effective and successful original research [39]. Research is valid when the conclusion is accurate and true, and research design is the conceptual blueprint used to conduct the research. Research design is the research structure, the glue that holds everything together [40]. This study's research design is based on the research model and the Game Theory, which provided a framework for the design.
2.4 Research Questions

To analyze the influence that perceived privacy concerns, perceived privacy risk, perceived control, and trust have on an individual's decisions to share personal information with organizations, this study seeks to explore the following research questions:

RQ. 1: Is there a statistically significant relationship between privacy control, privacy concerns, trust, and privacy risk, when an individual decides to share personal information with private or public organizations.

H1: Increased perceived privacy control reduces privacy concerns.
H2: Increased perceived privacy risk increases privacy concerns.
H3: Decreased trust increases privacy concerns.
H4: Increased perceived privacy control decreases perceived privacy risk.
H5: Perceived privacy control increases trust.
H6: Increased perceived privacy risk decreases trust.

The results showed that increased perceived privacy control reduces privacy concerns. The correlation is weak negative, which shows that these two variables move in the opposite direction; when the perceived privacy control decreases, the perceived privacy concerns increase. When the perceived privacy control increases, the perceived privacy concerns decrease. This is consistent with the literature review where [41] reported that when perceived privacy control decreases, the privacy concerns increase. The study was done on government surveillance as well as oversight, and 312 people completed the survey.

The results also showed that increased perceived privacy risk increases privacy concerns. In this case, the correlation is moderate positive, which means that when perceived privacy risk increases, the perceived privacy concerns also increase, so these two variables move in the same direction. This is also consistent with the literature review where [42] used the privacy calculus in the social media platform to analyze 354 survey responses, which indicated that perceived privacy risk is positively related to social privacy concerns.

The Pearson Correlation for this research question showed that decreased trust increases privacy concerns. The correlation is weak negative. These two variables move in the opposite direction; a decrease in trust will increase the perceived privacy concerns. An increase in trust will decrease the perceived privacy concerns. The results are consistent with the literature review. The correlational study done by [43] shows that trust and privacy concerns are direct predictors of patients’ behavior to accept technology in health services and disclose information. The study was done with 426 patients in New Delhi, India, and used structural equation modeling SEM to validate the hypotheses.

The privacy control and privacy risk, the results show that an increase in perceived privacy control decreases perceived privacy risk. The correlation is weak negative. These two variables move in the opposite direction; a decrease in the perceived privacy control will increase the perceived privacy risk. An increase in the perceived privacy control will decrease the perceived privacy risk. While the correlation in this study is negative weak, [44] drew a negative strong correlation between privacy control and privacy risk in the context of online social networks OSNs.

The perceived privacy control and trust, the results show that an increase of perceived privacy control will also increase trust. The correlation is moderate positive, and these two variables move in the same direction. The exact correlation is shown in the study [45] conducted with structural equation modeling SEM using survey data from Finland. The results indicate that trust increases when patients have control over their data; hence, the willingness to share personal health information PHI also increases.

The last hypothesis that was tested for the first research question was the correlation between perceived privacy risk and trust. The correlation is weak negative, which means that these two variables move in the opposite direction; a decrease in the perceived privacy risk will increase trust. An increase in the perceived privacy risk will decrease trust.
privacy risk will decrease trust. This is consistent with what was described in the literature review. In quantitative correlational study conducted by [46], there were 1399 valid questionnaires collected, and results showed that perceived trust correlated negatively with perceived privacy risk, consistent with what this research found too.

The Pearson Correlation results for this research question show only the relationship that exists among the variables chosen. Other factors were not included in this research question, which can affect the positive or negative correlation between each pair of the variables in the hypotheses. Despite the limitation of the correlation test, the results presented are consistent with the literature review.

RQ. 2: To what extent do privacy concerns vary by age, gender, and level of education in the decision-making process, when an individual decides to share information with private or public organizations.

H1: Perceived privacy concerns vary by age on the individual's decision to share personal information with various private or public organizations.

H2: Perceived privacy concerns vary by gender on the individual's decision to share personal information with various private or public organizations.

H3: Perceived privacy concerns vary by level of education on the individual's decision to share personal information with various private or public organizations.

This research question examined the effect that age, gender, and level of education had on perceived privacy concerns during the decision-making process of an individual deciding to share personal information with organizations. A one-way ANOVA test was run for the hypotheses in this research question. The results showed that age was the only independent variable that affects perceived privacy concerns. This is consistent with research done by [47], exploring perceived privacy concerns, trust, awareness, online data misuse, and self-efficacy regarding protective privacy measures. The research results indicated that older users significantly differ in their understanding of privacy issues and protect their data more actively than younger users. However, [48] argued a nonlinear relationship between age and information privacy concerns. In exploring the relationship between individuals' demographic characteristics and information privacy concerns IPC using panel data from the Korea Information Society Development Institute KISDI, a large sample from 7809 respondents was collected and analyzed. While the effects of level of education and income level were confirmed from the results, the impact of age and gender were not confirmed to have an influence on the privacy concerns.

The research question also indicates that gender and level of education do not affect perceived privacy concerns. However, other researchers have found that gender and education level influence privacy concerns. Gender differences in privacy concerns were examined by [49] across a wide array of Unmanned Aerial Systems UAS mission types. The results from 1067 responses indicated distinct gender male versus female differences in UAS privacy concerns. A larger sample of 9840 respondents in Korea was tested by [50]. ANOVA test showed the group differences of age, gender, and level of education followed by multiple regression analysis comparing the effects of each variable. The results indicated that men are more concerned about privacy than women. In addition to that, the results also showed that people with a higher level of education are more concerned about their privacy than people with lower education levels.

3. Implications for Future Study
Future studies should look deeper into the perceived effectiveness of the organizational privacy assurance mechanisms in each of the areas of e-commerce, e-government, and social networking. Specifically, future research studies should explore the tangible benefits that privacy mechanisms offer individuals, their clarity, and their design [51]. The privacy assurance mechanisms can either motivate the decision to share personal information, build trust, or create concerns and hesitation. Online retailers in e-commerce can find ways to influence the users by designing privacy assurance mechanisms that work. A privacy policy
should be clear and understandable for the consumers and should speak to the principles of collection, control, and usage of personal information [52]. The privacy policy should be placed in a conspicuous place on the website. It should have a periodic disclosure to the database of registered users to strengthen their positive beliefs. The privacy policy's communication is also essential, and it should be done during the registration process, and an email containing the information should be sent out. Creating a privacy policy is not good enough. The execution of that policy is what matters to the consumers.

A certification through external entities should be done to ensure privacy seals. Privacy seals are placed on websites; however, it will be of great value to research and examine e-government, social media, or e-commerce websites and the relationship of the privacy assurance mechanisms on these e-services with the laws and regulations like GDPR, HIPPA, and CCPA [53]. These regulations are put into place to protect the consumers’ personal data, so understanding these privacy mechanisms from the individual’s perspective and their needs is very important. It will help organizations boost the individuals’ trust in their privacy practices and differentiate them from the competitors. The awareness of protecting privacy is growing every day, so organizations can’t rely on privacy mechanisms that treat privacy as a checkbox. The data providers need and require more than that. It is beneficial for organizations to provide and practice the protection of personal information through mechanisms that work.

Taking each of the e-services domains as a separate study should be another direction for future research. The background problem can be the privacy paradox or some other behavior that can be researched even further. Some of the research areas in social networking can be people’s motivations to share personal information on these sites, the implications, and improvements that need to happen for personal data to be protected. E-commerce should be studied separately to see the flaws in the privacy assurance mechanisms and fulfill the needs of the consumers by protecting their data. Another aspect of e-commerce that can be explored is the laws and regulations applied and the improvements needed. E-government is another area that should be explored in future studies. The nature of the privacy concerns around personal data in this environment is different than the others. The amount of sensitive data that government agencies handle, and citizens’ surveillance are concerns and need to be addressed separately.

Finally, future studies should include the research that needs to be done in different regions other than the US and compare the results. Privacy is a multi-facet concept that involves culture, religion, regime, and various privacy laws. In Europe, GDPR has taken a more proactive approach than other countries to protect individual’s personal information. In the US, the need for a privacy law at the federal level is growing every day. Bringing these types of implications to life through research and future studies should be of great value and contribution to the body of knowledge.

4. Conclusion
Privacy is a fundamental individual right, and the individual’s personal information must be shielded from misuse, loss, or public scrutiny [54, 55, 56]. The right to privacy is often protected by laws in the US and other countries [57, 58]. The right to privacy is the right to autonomy [59]. It is the right of the individual to choose the entities, the purpose, the context, or the relationship under which an individual decides to share personal information [60]. This research study examined the effect of perceived privacy concerns, risk, control, and trust and the effectiveness of the organizational privacy assurance mechanisms on individuals’ decisions to share personal information. In the context of data mining techniques, the research model combined with Game Theory explained the individual's decision-making process and the factors that influence that process. The study's results showed a statistically significant relationship among the variables presented: perceived privacy concerns, perceived privacy risk, perceived privacy control, and trust. Demographics in this study were positioned as independent variables and helped to test individual’s privacy perceptions, trust, and behavior during the decision-making process.
This study indicates that future research of privacy concerns needs to be conducted in e-commerce, social networking, and e-government services. Each of these environments needs to be studied separately and present the findings that speak to that specific context. Demographics can be a subject for future studies to determine the specific attributes that affect an individual’s privacy perceptions, trust, and self-disclosure behavior. Perceived effectiveness of the organizational privacy assurance mechanisms in each of the areas of e-commerce, e-government, and social networking to be part of future research, given the fact that each of these areas handles different types of sensitive data, it has different needs for data and needs to comply with different privacy laws and regulations. Finally, taking the approach of exploring other regions and their privacy concerns, their perceptions, and their rules and regulations regarding privacy will bring different perspectives and analyses that can be a significant contribution in the privacy field.

References

[1] Chen, M.-Y., Yang, C.-C. & Hwang, M.-S., 2013. Privacy Protection Data Access Control. *International Journal of Network Security*, 15(6), pp. 411-419.

[2] Durnell, E., Okabe-Miyamoto, K., Howell, R. T. & Zizi, M., 2020. Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale. *International Journal of Human-Computer Interaction*, pp. 1-15.

[3] Farshadkhah, S., Van Slyke, C. & Fuller, J. B., 2020. Onlooker effect and affective responses in information security violation mitigation. *Computers & Security 100*.

[4] Sharma, S., Singh, G. & Pratt, S., 2021. Modeling the Multi-dimensional Facets of Perceived Risk in Purchasing Travel Online: A Generational Analysis. *Journal of Quality Assurance in Hospitality & Tourism*.

[5] Mutimukwe, C., Kolkowska, E. & Grönlunda, Å., 2020. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, 37(1).

[6] Libaque-Saenz, C. F. et al., 2016. The role of perceived information practices on consumers’ intention to authorise secondary use of personal data. *Behaviour & Information Technology*, 35(5), pp. 339-356.

[7] Mikalef, P., Boura, M., Lekakos, G. & Krogstie, J., 2019. Big data analytics and firm performance: Findings from a mixed-method approach. *Journal of Business Research*, pp. 261-276.

[8] Ristevski, B. & Chen, M., 2018. Big Data Analytics in Medicine and Healthcare. 5(3).

[9] Zou, H., 2016. Protection of Personal Information Security in the Age of Big Data. *IEEE*.

[10] Kanwal, T., Anjum, A. & Khan, A., 2020. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing*.

[11] Ebert, N., Ackermann, K. A. & Heinrich, P., 2020. Does Context in Privacy Communication Really Matter? — A Survey on Consumer Concerns and Preferences. *Human Factors in Computing Systems*.

[12] Kantarciglu, M. & Ferrari, E., 2019. Research Challenges at the Intersection of Big Data, Security and Privacy. *Frontiers in Big Data*.

[13] Barth, S. & D.T. de Jong, M., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), pp. 1038-1058.

[14] Kolotylo-Kulkarni, M., Xia, W. & Dhillon, G., 2020. Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, pp. 221-238.
Gómez-Barroso, J. L., 2021. Feel free to use my personal data: an experiment on disclosure behavior when shopping online. *Online Information Review*.

Farooq, M. & Qureshi, Q. A., 2020. Privacy of Internet Users in the Era of Transformative Marketing. *Journal of Management Practices, Humanities and Social Sciences*, pp. 25-28.

Soria-Comas, J. & Domingo-Ferrer, J., 2016. Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering*, pp. 21-28.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. & Saadi, M., 2017. Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, pp. 73-80.

Distler, V., Lallemand, C. & Koenig, V., 2019. How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*.

Gruschka, N., Mavroeidis, V., Vishi, K. & Jensen, M., 2018. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *IEEE*.

Zhao, B. et al., 2020. Anonymous and Privacy-preserving Federated Learning with Industrial Big Data. *IEEE*.

Reza, K. J., Estivill-Castro, V. & Islam, M. Z., 2017. Social media users' privacy against malicious data miners. *Research Gate*.

Cheng, X. et al., 2021. The good, the bad, and the ugly: impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*.

Lin, J., Carter, L. & Liu, D., 2021. Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems*.

Price, W. N. & Cohen, G. I., 2019. Privacy in the age of medical big data. *Nature Medicine*, pp. 37-43.

Puaschunder, J. M., 2018. Dignity and Utility of Privacy and Information Sharing in the Digital Big Data Age. *International Journal of Commerce and Management Research*, pp. 26-54.

Vannucci, V. & Pantano, E., 2020. Do I Lose my Privacy for a Better Service? Investigating the Interplay between Big Data Analytics and Privacy Loss from Young Consumers' Perspective. *Research Gate*.

Fortes, N., Rita, P. & Pagani, M., 2017. The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *International Journal of Internet Marketing and Advertising*.

Prince, C., 2018. Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, Volume 110, pp. 21-32.

Feng, Y., Yao, Y. & Sadeh, N., 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. pp. 1-16.

Mannhardt, F. et al., 2020. Trust and Privacy in Process Analytics. *International Journal of Conceptual Modeling*, Volume 15.

Metzger, M. J., 2017. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*.

Bansal, G., Zahedi, F., & Gefen, D., 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*.

Neumann, J. v. & Morgenstern, O., 1944. *Theory of Games and Economic Behavior*. s.l.:Princeton University Press.

Nash, J. F., 1950. Equilibrium Points in N-Person Games. *Proceedings of the National Academy of Sciences of the United States of America*, pp. 48-49.
[36] Shah, H., Kakkad, V., Patel, R. & Doshi, N., 2019. A survey on game theoretic approaches for privacy preservation in data mining and network security. Procedia Computer Science, pp. 686-691.
[37] Leedy, P. D., 2013. Practical Research: Planning and Design. 10th ed. Newmarket: Pearson.
[38] Newman, W. L., 2011. Social research methods : qualitative and quantitative approaches. 7th ed. Essex: Pearson.
[39] Mohajan, H. K., 2020. Quantitative Research: A Successful Investigation in Natural and Social Sciences. Journal of Economic Development, Environment and People.
[40] Akhtar, I., 2016. Research Design. Research Gate.
[41] Bansal, G. & Nah, F. F.-H., 2020. Measuring Privacy Concerns with Government Surveillance and Right-to-be-Forgotten in Nomological Net of Trust and Willingness-to-Share. Association for Information Systems.
[42] Jozani, M., Ayaburi, E., Ko, M. & Choo, K. K. R., 2020. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Computers in Human Behavior.
[43] Dhagarra, D., Goswami, M. & Kumar, G., 2020. Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective. International Journal of Medical Informatics.
[44] James, T. L. et al., 2017. Exposing others’ information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. Information & Management, pp. 851-865.
[45] Juga, J., Juntunen, J. & Koivumäki, T., 2021. Willingness to share personal health information: impact of attitudes, trust and control. Records Management Journal.
[46] Wang, E. S.-T. & Lin, R.-L., 2016. Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. Behaviour & Information Technology.
[47] Schomakers, E.-M., Lidynia, C., Vervier, L. & Ziefe, M., 2017. Online Privacy Perceptions of Older Adults. Research Gate.
[48] Lee, H., Wong, S. F., Oh, J. & Chang, Y., 2019. Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. Government Information Quarterly, pp. 294-303.
[49] Rice, S. et al., 2018. Public perception of UAS privacy concerns: a gender comparison. Journal of Unmanned Vehicle Systems.
[50] Lee, H., Wong, S. F. & Chang, L. Y., 2016. CONFIRMING THE EFFECT OF DEMOGRAPHIC CHARACTERISTICS ON INFORMATION PRIVACY CONCERNS. Research Gate.
[51] Jakovljević, M., 2017. Information Privacy: The Attitudes and Behaviours of Internet Users. Oeconomica Jadertina.
[52] Fortes, N., Rita, P. & Pagani, M., 2017. The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. International Journal of Internet Marketing and Advertising.[20] Gruschka, N., Mavroedis, V., Vishi, K. & Jensen, M., 2018. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. IEEE,[51] Jakovljević, M., 2017. Information Privacy: The Attitudes and Behaviours of Internet Users. Oeconomica Jadertina.
[53] Rothstein, M. A. & Tovino, S. A., 2019. California Takes the Lead on Data Privacy Law. The Hasting Center.
[54] Maurya, A. K., 2021. Privacy Rights during a Pandemic: A Comparative Study. Psychology and Education Journal, 58(2).
[55] Kayaalp, M., 2018. Patient Privacy in the Era of Big Data. Balkan Medical Journal, pp. 8-17.
[56] Kumar, M. & Kumari, P., 2020. Data Protection & Right to Privacy: Legislative Framework in India. *Journal of Critical Reviews*, 7(11).

[57] Abu, S., 2021. Right to Privacy, Data Protection and IOTs: An Appraisal of Legal Issues Covering Cross Border Data Transfer. *SSRN*.

[58] Nissim, K. & Wood, A., 2018. Is privacy privacy?.

[59] Becker, M., 2018. Ethics in the big data era: Privacy as autonomy and privacy as dignity. *Tydskrif vir Geesteswetenskappe*, pp. 669-682.

[60] Martiny, K. et al., 2021. Protecting Privacy during a Pandemic Outbreak. *International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pp. 308-318.

[61] M Dimodugno, S Hallman, Dept of Info Tech School CIS University of the Cumberlands, Williamsburg, KY USA, hallmandba@yahoo.com. M Plaisent and P Bernard Dept. Management and Technology, University of Quebec in Montreal, Canada, Michel.plaisent@uqam.ca.