Journal of Digital Convergence
Vol. 17. No. 11, pp. 149-156, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.11.149

Meta-Analysis of Information Privacy Using TSSEM

Jongki Kim
Professor, Dept. of Business Administration, Pusan National University

TSSEM을 이용한 정보 프라이버시 메타분석

김종기
부산대학교 경영학과 교수

Abstract With widespread use of information technologies, information privacy issues have been gaining more attention by not only the public but also researchers. The number of studies on the issues has been increasing exponentially, which makes incomprehensible the whole picture of research outcome. Thus, it is necessary to conduct a systematic examination of past research. This study developed two competing models with four essential constructs in information privacy research and empirically tested the models with data obtained from previous studies. This study employed a quantitative meta-analysis method called TSSEM. It is one of MASEM methods in which structural equation modeling and meta-analysis are integrated. The analysis results indicated that risk-centric model exhibited much better model fits than those of concern-centric model. This study implies that traditional concern-centric model should be questioned it's explanatory power of the model and researchers may consider alternative risk-centric model to explain user's intention to provide privacy information.

Key Words : Information Privacy, Meta-analysis, TSSEM, Concern-centric Model, Risk-centric Model

요 약 정보기술의 활용이 보편화되면서 대중과 연구자 모두 정보 프라이버시 문제에 대한 관심이 높아지고 있다. 이러한 문제에 대한 연구가 기하급수적으로 증가하면서 연구결과에 대한 전반적인 이해가 어려워졌다. 이에 따라 과거 연구에 대한 체계적인 검토가 요구된다. 본 연구는 정보 프라이버시 연구에 핵심적인 네 가지 연구개념을 두 가지 연구모형으로 설정하고 기존 연구에서 수집된 데이터를 이용하여 실증 분석하였다. TSSEM이라는 정량적 메타분석 기법이 적용되었는데, 이 기법은 MASEM의 한 가지로서 구조방정식모형과 메타분석 기법을 통합하여 분석하는 기능을 제공한다. 분석결과는 위험 중심적 모형이 염려 중심적 모형과 비교하여 보다 높은 모형 적합도를 나타내었다. 본 연구의 결과는 전통적인 염려 중심적 모형의 설명력에 의문을 제시하며, 사용자의 프라이버시 정보 제공의도를 설명하기 위하여 위험 중심적 모형을 고려할 필요가 있다는 점을 시사한다.

주제어 : 정보프라이버시, 메타분석, 이단계구조방정식, 염려중심모형, 위험중심모형

1. Introduction

No one can deny that privacy is one of the basic human rights. Rapid advancement of information technology enables collection, distribution and use of personal information

*This study was supported by the Fund for Humanities & Social Studies at Pusan National University 2018.
*Corresponding Author : Jongki Kim(jkkim1@pusan.ac.kr)
Received October 2, 2019 Revised October 31, 2019
Accepted November 20, 2019 Published November 28, 2019

much easier than before. In the every corner of the world, users are expressing concerns on information privacy as human life is more dependent on information technologies[1].

Understanding how users perceive the issues on information privacy and react to keep their privacy rights are one of the major research interests. The number of studies on information privacy has been increasing exponentially, which causes difficulties in comprehending the overall picture of research trend. There has been several studies reviewing current status of information privacy research and provided clear views on vast landscape of the research area. However, most of review studies are based on qualitative literature review.

Many studies proposed and empirically tested causal models which attempted to explain relationships among various constructs. Majority of research models use a construct named 'information privacy concerns' as a central concept of models and investigate relationships with other related constructs.

This study aims to identify essential elements of information privacy research and to show how those elements are related. This study also develops, meta-analytically compares and tests two distinctive perspectives on information privacy. While most of past literature review research have synthesized prior studies with qualitative methods, this study attempts to quantitatively test the research model.

2. Meta-Analysis on Information Privacy

Information privacy concerns privacy issues in the digital context. The number of research on information privacy has been dramatically increased as the world society entered into digital era with the development of information and communication technologies[2]. As the information privacy research accumulates, it needs to produce cumulative knowledge by comparing and combining research findings across vast amount of prior research.

There are several methods to achieve comprehensive understanding by synthesizing research findings. Before 1990s, narrative review method was widely used. It often involves using convenient sampling, narrative description about studies, and vote counting[3]. This method is criticized for lack of objectivity and transparency. It is also difficult to conduct as more research are available.

Systematic literature review and meta-analysis were introduced to overcome the limitations of traditional narrative review method. Both methods are devised to acquire transparent and reproducible results by analyzing prior research outcomes systematically and comprehensively[3]. While the systematic literature review aims on a qualitative synthesis of qualitative or quantitative studies, the meta-analysis focuses on quantitative integration of quantitative research findings[4].

Meta-analysis is a statistical method to synthesize the effect sizes of various research findings. A meta-analysis uses summary statistics (i.e., effect size statistics) such as mean difference, correlation coefficient, or odds ratio[5]. Meta-analysis has several advantages over individual research. It can improve precision and accuracy of estimates which affect greater statistical power[29,30].

Structural equation modeling (SEM) has become extremely popular in most, if not all, of social science area[6]. It is a method that combines confirmatory factor analysis and multiple regression or path analysis. While covariance-based structural equation modeling (CB-SEM) was introduced earlier, partial least squares structural equation modeling (PLS-SEM) was getting more attention recently.

Combining meta-analysis and structural equation modeling can provide better model fit and stable parameter estimates because the

analysis is based on much larger sample size than that of each study[7]. It is also possible to create and test new model which is not in the prior individual research[5].

Meta-analytic structural equation modeling (MASEM) requires a pooled correlation coefficient matrix to perform SEM analysis and uses Pearson correlations, Fisher's z scores, or generalized least squares for pooling correlation matrix[6]. Cheung and Chan[8] proposed a two-stage structural equation modeling (TSSEM) method. They claims that TSSEM provides a unified framework to integrate meta-analysis and SEM[8].

There are several studies on information privacy based on the traditional narrative review or the systematic literature review method. Smith et al.[9] reviewed a large number of privacy-related research to understand the concept of information privacy, relationships between information privacy and other constructs, and the contexts of these relationships. They proposed APCO(Antecedents-Privacy Concerns-Outcomes) Macro Model in which depicted the privacy concerns as a central construct.

Li[10] conceptualized privacy concerns as two types (general and specific) and proposed an Integrative Framework in which various constructs were related to those two types of concerns. Li[11] identified 12 theories used to explain online information privacy research and depicted an integrated framework based on dual-calculus perspective. Dinev et al.[12] revised Smith et al.[9]'s APCO model to incorporate new perspectives such as behavioral economics and psychology (i.e., elaboration likelihood model).

Gerber et al.[1] conducted a literature search to identify articles on privacy paradox. They revealed several key factors in explaining privacy paradox and listed effect sizes of variables used in the studies.

Yun et al.[2] chronologically reviewed research on information privacy concerns. They found out that the number of studies as well as the constructs used in the research has increased dramatically. Also, the contexts of research has changed from general to specific ones.

Some studies performed a comprehensive literature review on privacy paradox phenomenon which refers to the inconsistency of privacy attitude and intention. Kokolakis[13] provided interpretations of the privacy paradox based on five theories. After reviewing 32 papers, Barth and De Jong[14] asserted that rational decision-making based on risk-benefit calculus perspective was not enough to explain privacy paradox.

3. Research Model

Jia et al.[15] proposed and empirically tested two contrasting research models to understand processes of privacy risk-taking and risk-coping behaviors in the use of social media. One is the concern-centric model, as shown in Fig. 1, which is based on APCO model.

Smith et al.[9] investigated the relationships between privacy and other constructs. They posited privacy concern as the central concept and found several variables, such as privacy experiences, privacy awareness, personality differences, demographic differences, and culture, influenced users' privacy concern. They identified behavioral reactions as the main outcome of privacy concern. Behavioral reactions also influenced by privacy calculus factors as well as trust factor. One interesting notion of their model was that trust and regulation were reciprocally related to privacy concern. Li[11] viewed trust as a part of risk calculus process to decide the need for privacy. It, in turns, was an element of privacy calculus for disclosure intention of privacy information.

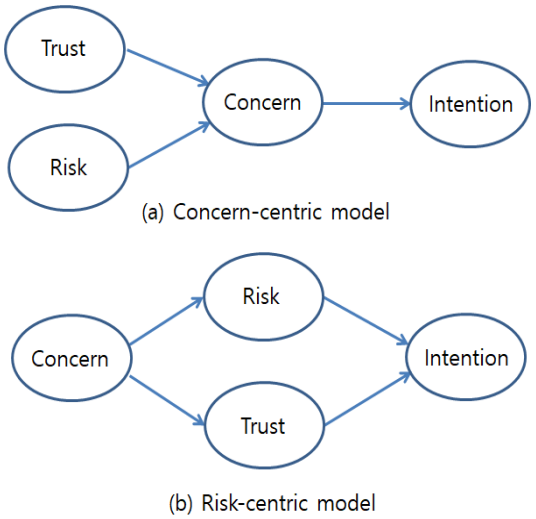

Fig. 1. Research Models

While the concern-centric model assumes rational privacy choices according to the concern for information privacy, risk-centric model focuses on risk-aversion behavior due to bounded rationality[15]. The risk-centric model emphasizes the influence of risk perception and trust propensity on intention to provide personal information. The privacy concern plays as an antecedent to risk and trust. Smith et al.[9] found that privacy concern had indirect relationship with intention where trust and risk were mediating variables.

Both models consist of four constructs which are considered essential variables to understand user's information privacy behavior. Risk and trust are two important factors in the decision of privacy intention. Dinev et al.[12] included trust and risk as major factors in the Enhanced APCO Model. Li[10] also posited that trust and risk were essential elements of the Integrative Framework on CFIP(Concerns For Information Privacy). In the framework, trust belief and perceived privacy risks played mediating roles for influence of specific CFIP on behavioral intention.

Zhou[16] also modeled user's privacy concern on location-based services from risk-centric perspective.

The concept of privacy concerns has been extensively researched. Smith et al.[9] established a measurement model for CFIP based on 15 measuring items. They proposed a multidimensional construct of privacy concerns that consisted of collection, error, unauthorized secondary use and improper access.

Malhotra et al.[17] classified information privacy concerns on Internet environment into three aspects; namely, collection, control and awareness. Dinev and Hart[18] synthesized CFIP[9] and Culnan and Amstrong[19]'s study and proposed a measurement model called information privacy concern(IPC) in the Internet context. They measured IPC by user's awareness level of abuse and finding.

Another type of research on privacy concerns is whether the context is general or specific. General privacy concern is user's overall assessment of feeling on how his/her privacy information would be handled. Factors such as level of self-esteem, perceived risk and computer anxiety have significant predictive value on general privacy concern[1].

Website reputation has direct impact on specific privacy concern. Type of privacy information (e.g., medical information) as well as context of privacy information usage (e.g., SNS) were also found to have significant impact[1,15,20].

Intention to provide privacy information is considered as an appropriate proxy for actual behavior based on the Theory of Planned Behavior. Numerous research have been conducted in accordance with this notion. 'Intention' has been investigated in different context such as SNS, location-based services and online shopping[1].

Some studies showed that there was unclear relationship between concerns and trust. Smith et al.[9] posited that trust had a bidirectional relationship with privacy concerns. Dinev et al.[12] also depicted the relationship in the same way as Smith et al.[9].

4. Data Analysis

4.1 Data

Identifying studies to perform a meta-analysis requires extensive efforts. It begins with searching academic databases with relevant keywords. Initially identified articles are evaluated based on predetermined criteria such as use of certain analysis methods, quality assessment of study, time period, etc.

This study utilized the data reported in Gerber et al.[1]. They[1] performed a systematic literature review to identify studies on information privacy. Their main focus was on privacy paradox, but their study encompassed most of major variables in the information privacy research. They began literature identification process with the 'privacy paradox' keyword search in several databases such as Google Scholar, ACM Digital Library, IEEE Xplore Digital Library and Scopus. Initial search resulted in 181 articles. Among them, Gerber et al.[1] included only those studies which performed empirical research with regression analysis or SEM. Thirty-eight studies were remained after performing a series of scrutinizing procedure.

Quality assessment on the included studies were conducted according to the quality criteria proposed by Malhotra and Grover[21]. They also performed power analyses with G*Power and Free Statistics Calculators. All studies yielded above 0.8 and no study deleted due to insufficient statistical power Gerber et al.[1].

Correlation coefficients among constructs in the research model are required to conduct an analysis with TSSEM. Among 38, 14 studies reported correlation coefficient matrix among research variables. Several studies[22-26] included more than one correlation coefficient between two research constructs. For example, Keith et al.[22] decomposed privacy risk into two specific risks; namely, location data risk and personal information risk. Considering multiple correlations among constructs, this study identified 23 correlation coefficient matrices with total sample of 10,889.

4.2 Analysis and Discussion

This study employed TSSEM proposed by Cheung and Chan[8]. The metaSEM package was used to analyze the research models. It is a MASEM tool based on OpenMx package in R programming platform[27].

Stage 1 of TSSEM begins with pooling correlation matrices. It needs to be decided whether to use fixed effects model (FEM) or random effects model (REM)[31]. FEM assumes that all differences among correlation coefficients are due to sampling errors. Then, it is not possible to extend any inferences beyond studies included in the sample. On the other hand, REM takes variances among studies into account. Therefore, it is possible to extend any inferences into more general situation[6].

The tssem1() function in the metaSEM is used to analyze whether to use FEM or REM[5]. The χ^2 of FEM with equal correlation coefficients on all studies in the sample was significant $\chi^2_{(51)} = 653.73$ with $p < 0.05$. RMSEA was 0.158 which is larger than cutoff value of 0.08. Therefore, it is not recommended to use FEM in stage 2 of TSSEM. The Q statistic of REM was significant ($Q_{(51)} = 536.23$, $p < 0.05$), which indicated significant heterogeneity in the data.

Stage 2 of TSSEM specifies the structural model. For the concern-centric model, RMSEA was 0.085 with 95% confidence interval of (0.074, 0.096). CFI of 0.79 also indicated marginally acceptable fit of the model with cutoff value of larger than 0.90. All of the path coefficients in the model were significant at $p < 0.05$ as shown in Table 1.

Table 1. Path Coefficients of Concern-centric Model

Path	Estimate	z-value	p-value
Trust -> Concern	-0.61	-17.02	< 0.001
Risk -> Concern	0.23	3.29	< 0.01
Concern -> Intention	-0.68	-22.34	< 0.001

The risk-centric model exhibited adequate fit of the model. RMSEA was 0.019 with 95% confidence interval of (0.008, 0.031) and CFI was 0.99. Table 2 shows that all path coefficients of the model are significant.

Table 2. Path Coefficients of Risk-centric Model

Path	Estimate	z-value	p-value
Concern -> Trust	-0.29	-6.35	< 0.001
Concern -> Risk	0.37	6.96	< 0.001
Trust -> Intention	0.54	22.66	< 0.001
Risk -> Intention	-0.25	-5.26	< 0.001

Although all path coefficients of both models were statistically significant, the fit indexes of risk-centric model indicated that it was better than the concern-centric model to explain the variance of data. This result is in accordance with Jia et al.[15]'s finding. They empirically tested two models and confirmed that the risk-centric model exhibited a much better fit to the data.

The concern-centric model alone can be acceptable to explain user's intention to provide privacy information. However, risk-centric model exhibits much higher model fits when two models are compared. This implies that it is better to posit risk and trust as mediator variables between privacy concerns and intention.

5. Conclusions

With heightened concerns on information privacy, much research has been done on various issues of information privacy. As more studies accumulated, it is hard to figure out the whole picture of research trends. Several studies have been conducted to understand various aspects of research in information privacy, but all of them are based on qualitative methods.

This study investigated how users decide to provide privacy related information. Four essential constructs were identified based on previous studies. Specifically, two contrasting views, concern-centric model and risk-centric model, were modeled and empirically tested with one of the quantitative meta-analysis methods called TSSEM. It is an analytical method to combine meta-analysis and SEM in a coherent manner. The analysis results showed that, while all of the paths in both models were significant, the model fit indexes of risk-centric model were much better than those of concern-centric model.

SEM gains a great popularity among researchers not only in information privacy but also other topics. CB-SEM as well as PLS-SEM are commonly used methods and some researchers consider them interchangeable, although theoretical background and purpose of each method are quite different[28]. One interesting implication of this study is the choice of analysis method. If one uses PLS-SEM for the concern-centric model, the model would be accepted without any problem because of the statistical significance of all paths in the model. On the other hand, CB-SEM would clearly indicate problems of model fit in the concern-centric model because CB-SEM method focuses on overall explanation of variance in the data by the model. Therefore, it is important to choose appropriate analysis method for research purpose.

The data used in this study is based on the data collected in Gerber et al.[1]. Although Gerber et al.[1] performed data extraction procedure systematically, it is possible to include

more data by expanding timeline, using more keyword, or adding other analytical methods.

There are several other constructs identified in the studies proposing integrative models[9-12]. Extended model including constructs other than those in this study can be meta-analyzed. It is also possible that a meta-analysis can be performed on specific topics such as privacy paradox, behavioral economics in information privacy, privacy calculus, etc.

REFERENCES

[1] N. Gerber, P. Gerber & M. Volkamer. (2018). Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security, 77,* 226-261. DOI: 10.1016/j.cose.2018.04.002

[2] H. Yun, G. Lee & D. J. Kim. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56(4),* 570-601.

DOI: 10.1016/j.im.2018.10.001

[3] S. Whang. *Meta-Analysis Using R,* Hakjisa, 2015.

[4] C. Okoli. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems, 37,* 879-910. DOI: 10.17705/1cais.03743

[5] S. Jak. (2015). *Meta-analytic structural equation modeling*. New York: Springer. DOI: 10.1007/978-3-319-27174-3

[6] M. W. L. Cheung. (2015). *Meta-analysis: A structural equation modeling approach.* John Wiley & Sons.

[7] R. S. Landis. (2013). Successfully Combining Meta-analysis and Structural Equation Modeling: Recommendations and Strategies. *Journal of Business and Psychology, 28(3),* 251-261. DOI: 10.1007/s10869-013-9285-x

[8] M. W. L. Cheung & W. Chan. (2005). Meta-Analytic Structural Equation Modeling: A Two-Stage Approach. *Psychological Methods, 10(1),* 40-64. DOI: 10.1037/1082-989x.10.1.40

[9] H. J. Smith, T. Dinev & H. Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35(4),* 989-1016. DOI: 10.2307/41409970

[10] Y. Li. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *CAIS, 28,* 28. DOI: 10.17705/1cais.02828

[11] Y. Li. (2012). Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. *Decision Support Systems, 54(1),* 471-481. DOI: 10.1016/j.dss.2012.06.010

[12] T. Dinev, A. R. McConnell & H. J. Smith. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research, 26(4),* 639-655. DOI: 10.1287/isre.2015.0600

[13] S. Kokolakis. (2015). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security, 64,* 122-134. DOI: 10.1016/j.cose.2015.07.002

[14] S. Barth & M. D. De Jong. (2017). The privacy paradox-Investigating discrepancies between expressed privacy concerns and actual online behavior-A systematic literature review. *Telematics and Informatics, 34(7),* 1038-1058. DOI: 10.1016/j.tele.2017.04.013

[15] H. Jia, P. J. Wisniewski, H. Xu, M. B. Rosson & J. M. Carroll. (2015, February). Risk-taking as a learning process for shaping teen's online information privacy behaviors. *In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 583-599). ACM. DOI: 10.1145/2675133.2675293

[16] T. Zhou. (2015). Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors. *Information Systems Frontiers, 17(2),* 413-422. DOI: 10.1007/s10796-013-9413-1

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

[18] T. Dinev & P. Hart. (2004). Internet Privacy Concerns and Their Antecedents-Measurement Validity and a Regression Model. *Behaviour & Information Technology, 23(6),* 413-422. DOI: 10.1080/01449290410001715723

[19] M. J. Culnan & P. K. Armstrong. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust : An Empirical Investigation. *Organization Science, 10(1),* 104-115. DOI: 10.1287/orsc.10.1.104

[20] M. Koohikamali, N. Gerhart & M. Mousavizadeh. (2015). Location disclosure on LB-SNAs: the role of incentives on sharing behavior. *Decision Support Systems, 71,* 78-87. DOI: 10.1016/j.dss.2015.01.008.

[21] M. K. Malhotra & V. Grover. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of Operations Management, 16(4),* 407-425. DOI: 10.1016/s0272-6963(98)00021-7

[22] M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry & C. Greer. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies, 71(12),* 1163-1173. DOI: 10.1016/j.ijhcs.2013.08.016

[23] Y. Li. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications, 13(1),* 32-44. DOI: 10.1016/j.elerap.2013.08.002

[24] C. L. Miltgen & H. J. Smith. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52(6),* 741-759. DOI: 10.1016/j.im.2015.06.006

[25] K. S. Schwaig, A. H. Segars, V. Grover & K. D. Fiedler. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50(1),* 1-12. DOI: 10.1016/j.im.2012.11.002

[26] H. Xu, H. H. Teo, B. C. Tan & R. Agarwal. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research, 23(4),* 1342-1363. DOI: 10.1287/isre.1120.0416

[27] M. W. L. Cheung. (2015). metaSEM: An R package for meta-analysis using structural equation modeling. *Frontiers in Psychology, 5,* 1521. DOI : 10.3389/fpsyg.2014.01521

[28] E. E. Rigdon (2016). Choosing PLS path modeling as analytical method in European management research: A realist perspective. *European Management Journal, 34(6),* 598-605. DOI: 10.1016/j.emj.2016.05.006

[29] K. H. Kim (2016). A Convergence Study about Meta-Analysis on the Effects of ACT Intervention Program. *Journal of the Korea Convergence Society, 7(5),* 145-153. DOI: 10.15207/JKCS.2016.7.5.145

[30] S. H. Hwang, H. C. Jeong & J. W. Hwang. (2019). Effect of Laughter Therapy on Healthy Life: A Meta-analysis. *Journal of the Korea Convergence Society, 10(9),* 291-299. DOI: 10.15207/JKCS.2019.10.9.291

[31] B. Cho & J. Lee. (2018). A Meta Analysis on Effects of Flipped Learning in Korea. *Journal of Digital Convergence, 16(3),* 59-73. DOI: 10.14400/JDC.2018.16.3.059

김 종 기(Jongki Kim) [정회원]

· 1987년 2월 : 부산대학교 경영학과 (경영학사)
· 1988년 12월 : 미국 아칸소 주립대 경영대학원(경영학석사)
· 1992년 12월 : 미국 미시시피 주립대 경영학과(경영학박사)
· 1999년 3월 ~ 현재 : 부산대학교 경영학과 교수
· 관심분야 : 정보 프라이버시, 정보보안, 연구방법론, 기술혁신
· E-Mail : jkkim1@pusan.ac.kr