Nam, Sangjun; Kwon, Youngsun

Conference Paper

The impact of the strengthened personal data protection regulation on users' privacy concerns

24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Nam, Sangjun; Kwon, Youngsun (2024) : The impact of the strengthened personal data protection regulation on users' privacy concerns, 24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/302472

The impact of the strengthened personal data protection regulation on users' privacy concerns

Sangjun Nam[a, b, *], Youngsun Kwon[b, †]

[a] Technology Policy Research Division,
Electronics and Telecommunications Research Institute,
218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, Republic of Korea

[b] School of Business and Technology Management, College of Business, KAIST,
291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

Keywords: Personal Data, Online Platform, Regulation, Privacy Concern, App Tracking Transparency

Abstract

Considering that privacy concerns could affect users' privacy behavior as an antecedent, it is important to investigate the impact of strengthened personal data protection regulation on users' privacy concerns. However, there exists mixed views that the personal data protection regulation has a positive or negative effect on users' privacy concerns by increasing privacy awareness and trustworthiness, respectively. We propose the approach using smartphone platform-level privacy regulation as a proxy for national-level personal data protection regulation to overcome the difficulty of setting up treatment and control groups for implementing dynamic Difference-in-Difference analysis. The result showed that introducing personal data protection regulation has a positive effect on users' privacy concerns in the short term; however, the positive effect could be diluted over time.

1. Introduction

Collecting users' personal data is common in exchange for various purposes on online platforms, and the personal data is used for monetizing and attracting more users. Therefore, online platforms have an incentive to collect personal data from users excessively. In this regard, privacy concerns are also increasing due to the excessive collection. Against this background, personal data protection regulations began to be introduced, starting with the European Union's (EU's) General Data Protection Regulation (GDPR). Personal data protection regulations such as the GDPR aim to protect the rights of information privacy while not excessively decreasing the efficiency of data-based businesses (Bauer et al., 2022). Therefore, it is important to shed light on the impact of the strengthened personal data protection regulation on users' privacy concerns because users' privacy concerns affect the firm's capabilities of collecting personal data negatively by discouraging users' willingness to share personal data.

However, capturing the effect of personal data protection regulations is not simple. One general approach to investigating the causal effect of policies is measuring the average treatment effects on the treated (ATT) with Difference-in-Difference (DID). Bauer et al. (2022) used the GDPR awareness concept to classify respondents into the treatment group and control group to measure the effect of GDPR with DID analysis. However, they did not find any significant results

* sjnam@etri.re.kr
† yokwon@kaist.ac.kr

for some reason, such as insufficient awareness of the actual stipulation of the regulation. This insignificant result implies that it is difficult to set up treatment and control groups to measure the causal effect of personal data protection regulation using DID.

To address this research gap, we propose the approach of using smartphone platform-level personal data protection regulations as the proxy for national-level privacy regulations. Considering that smartphone platforms play a privacy regulator role based on their intermediate function as the 'platforms of platforms' (Van Hoboken & Fathaigh, 2021), we assumed that the strengthened privacy policy at the platform level could be a proxy of the strengthened personal data protection regulation at the national level. Moreover, smartphone users could be more easily aware of platform-level privacy regulations than national-level privacy regulations. For example, the iOS privacy policy, App Tracking Transparency (ATT), asks iOS users to explicit consent to track their personal data in each app when they use the app for the first time. Thus, iOS users can be aware of the functions of ATT relatively easily. In this approach, the effect of platform-level privacy regulations on users' perceptions can be estimated by classifying users based on their smartphone platforms.

Previous studies have mixed views on the impact of the privacy regulation on users' privacy concerns. The strengthened personal data protection regulation may decrease users' privacy concerns by improving the trustworthiness related to data collectors (Wu et al., 2012; Fox et al., 2022; Bauer et al., 2022). On the other hand, the strengthened personal data protection regulation may positively affect users' privacy concerns by improving privacy awareness (Bergmann, 2008; Benamati et al., 2017; Schaub et al., 2016). In this background, we expect that our study provides some meaningful implications for both academics and regulators by shedding light on this gray area.

The remainder of this paper is organized as follows. Section 2 reviews previous studies on the concept of information privacy and information privacy concerns. It also reviews previous studies that investigated the relationship between personal data regulations and information privacy concerns, and the platform-level privacy policy. Section 3 presents this study's research methodology and data. Section 4 reports and interprets the empirical findings. Finally, Section 5 discusses the implications.

2. Literature Review

2.1. The concept of information privacy and information privacy concerns

This paper aims to investigate the relationship between strengthened personal data protection regulations and users' privacy concerns. To discuss the relationship between regulation and privacy concerns, we started by exploring the concept of information privacy and the importance of information privacy concerns in the context of personal data collection on online platforms. Information privacy, a subset of whole privacy concepts, concerns access to individually identifiable personal data (Smith et al., 2011). From this perspective, many researchers have noted that information privacy is related to controlling personal data collection and use (Stone & Stone, 1990; Hann et al., 2007; Bélanger & Crossler, 2011). Therefore, it can be viewed that users worry about personal data collection on online platforms in terms of information privacy. This individual's concern regarding their information privacy refers to information privacy concerns (Smith et al., 1996). Dinev and Hart (2006) described that privacy concerns are beliefs about who has access to their disclosed personal information via the Internet and how it is utilized. Thus, privacy concerns are increased due to the uncertainty of access and use of personal data (Dinev & Hart, 2006). In summary, users' perceptions related to collecting personal data on online platforms can be measured by information privacy concerns (Smith et al., 2011).

Information privacy concerns are one of the key concepts explaining the users' information privacy behaviors (Bélanger & Crossler, 2011; Smith et al., 2011). Previous findings suggest that

information privacy concerns influence individuals' privacy attitudes as well as acceptance of technology and services in various contexts (Dienlin & Metzger, 2016; Dinev & Hart, 2006; Fox et al., 2021; Malhotra et al., 2004; Van Slyke et al., 2006). This implies that the high level of information privacy concerns has a negative impact on the data-driven industry by discouraging users' acceptance of data-based services and their willingness to share personal data. Considering that personal data protection regulations such as the GDPR aim to protect the rights of information privacy while not excessively decreasing the efficiency of data-based business (Bauer et al., 2022), it is important to investigate the impact of strengthened personal data regulation on users' information privacy concerns.

2.2. The personal data protection regulation and information privacy concerns

For users, personal data regulation such as the General Data Protection Regulation (GDPR) is the regulation ensuring users' rights of control and choice to access and use their personal data. The GDPR aims to clarify, codify, and extend individual data rights (Bauer et al., 2022). In a similar vein, the Personal Data Protection Act has been devised to ensure notification and consent before collecting and utilizing users' personal data in South Korea. Therefore, the impact of strengthened personal data protection regulation affects users' information privacy concerns by changing users' perceptions related to the collection and use of personal data.

However, it is uncertain whether the strengthened regulation affects users' information privacy concerns negatively or positively. It seems natural that the negative relationship between the strengthened personal data protection regulation and information privacy concerns by providing proper information related to information privacy (LaRose and Rifon, 2006; Rifon et al., 2005; Wang et al., 2004). Wu et al. (2012) investigated the relationship between the online privacy policy and privacy concerns. The authors found that the five dimensions of privacy policy, such as notice, choice, access, security, and enforcement, have a negative relationship with privacy concerns and/or a positive relationship with trust. Bauer et al. (2022) expected that the awareness of GDPR positively affects users' trust in data collectors because they can expect that data collectors will not misuse their data to comply with the GDPR. Fox et al. (2022) also found that the GDPR label affects users' trustworthiness positively. Considering the negative relationship between privacy concerns and trust (Bélanger & Crossler, 2011; Smith et al., 2011; Swani et al., 2021), the strengthened personal data protection regulation eases users' privacy concerns by enhancing trust.

On the other hand, the strengthened personal data protection regulation may positively affect users' information privacy concerns by increasing privacy awareness. Privacy awareness refers to the degree to which individuals are aware of organizations' privacy practices (Ozdemir et al., 2017; Smith et al., 2011). Under the "Antecedents – Privacy Concerns – Outcomes" (APCO) framework, which Smith et al. (2011) suggested, privacy awareness has a positive relationship with privacy concerns as an antecedent of privacy concerns (Benemati et al., 2017; Ozdemir et al., 2017). Users' privacy awareness can be improved due to the strengthened personal data protection regulation by providing knowledge related to the practices of collecting personal data. In this context, Bergmann (2008) found a positive relationship between privacy policy and privacy awareness. In line with these previous findings, Schaub et al. (2016) empirically showed that the new awareness of the prevalence of tracking gained through the browser extension that provides information about the tracking of personal data could increase users' privacy concerns. Similar to the privacy policy at the service level, Fox et al. (2022) found that the GDPR privacy label affects users' perception of privacy. In summary, strengthened personal data protection regulations may positively affect users' privacy concerns by improving their privacy awareness.

Previous findings suggest that the effect of the strengthened personal data protection regulation on users' privacy concerns can vary depending on the degree of improved privacy awareness and trustworthiness. In the short run, the regulation may have a positive effect on privacy concerns due to the improved privacy awareness, considering that users newly recognize the prevalence of collecting personal data when the regulation is introduced. In the long-term, the increased privacy concerns can be diluted by improving the trustworthiness of data collectors, which will provide proper information and options to comply with the regulation. Bauer et al. (2022) noted that personal data protection regulations such as the GDPR may have the long-term effect. Thus, it may be meaningful to investigate the dynamic effect of the strengthened personal data protection regulation on users' privacy concerns.

2.3. The platform-level privacy policy as a proxy of the personal data protection regulation

As noted in the previous section 2.2, the strengthened personal data protection regulation affects users' perceptions of privacy, such as trust and privacy awareness. However, it is not easy to measure the causal effect of the regulation on users. Bauer et al. (2022) attempted to measure the effect of GDPR on users' trust in data collectors using the awareness of GDPR. However, they did not find statistically significant evidence. The authors noted that the insufficient awareness related to the actual stipulation of personal data regulation could be one of the possible explanations for this insignificant result. To address this research gap, we consider the platform-level privacy policy as a proxy of the personal data protection regulation.

Smartphone platforms such as Apple and Google are perceived as 'platforms of platforms' on other platforms (Nooren et al., 2018). Van Hoboken and Fathaigh (2021) explained that these platforms act as regulators based on the intermediate function accompanied by a rule-setting feature. In line with this context, they argued that the smartphone platforms that find themselves in a role as privacy regulators are introducing platform-level privacy regulations. In April 2021, Apple introduced App Tracking Transparency (ATT), requiring iOS apps to ask users for explicit permission before tracking. Under the ATT, the app can access the Identifier for Advertisers (IDFA), a random and unique identifier provided by the operating systems (OS) to apps for tracking users in the OS, only if an iOS user consents to track (Kollnig et al., 2022). The fact that the introduction of ATT affects all users, as well as app developers in iOS, is similar to the fact that certain countries' personal data protection regulations affect all users and data collectors in that country. In this background, we assumed that the ATT, a newly introduced platform-level privacy policy, can be a proxy for the strengthened personal data protection regulation to investigate the impact of the regulation on users' privacy concerns.

Using the introduction of ATT as a proxy for the strengthened personal data protection regulation has some advantages. First, users are easily aware of the change in the privacy policy in iOS because ATT asks users for explicit consent with a pop-up notice. This means that users were exposed to ATT repeatedly when they used each app for the first time after the iOS update. Thus, users are relatively easily aware of the change in privacy policy compared to the national level personal data protection regulation. Second, it is easy to divide users into the treatment group and the control group based on their smartphone device. In this case, iPhone users are classified as part of the treatment group, and non-iPhone users are classified as part of the control group because non-iPhone users never experience ATT.

3. Methodology and Data

This study uses the dynamic difference-in-differences (dynamic DID) approach, the so-called event study analysis, to investigate the causal effect of the ATT on iOS users' information privacy concerns with multiple time periods. We used the Callaway-Sant'Anna Difference-in-Difference (CSDID) methods (Callaway & Sant'Anna, 2021)

with STATA csdid package.

To implement the CSDID methods, we use the Korean Media Panel Survey data provided by the Korea Information Society Development Institute (KISDI) yearly since 2010. These datasets are useful for this study because they contain measures of privacy concerns, smartphone devices, digital capabilities related to protecting privacy, and demographic characteristics. The post-treatment period is set after April 2021 based on the introduction of the ATT in South Korea with the iOS update. The period of data is set from 2017.6 to 2023.6 following the fact that the survey of the KISDI media panel is conducted every June, as shown in Figure 1.

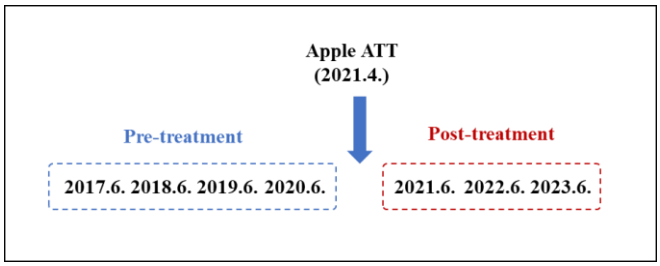

Figure 1. Data period

As mentioned in section 2.3., the iOS users who experience the ATT are in the treatment group, and the other users who never experience the ATT are in the control group. More specifically, we label people who continue to use iPhones after 2020 to the treatment group and others who have not used an iPhone since 2020 to the control group for capturing the dynamic causal effect of ATT since the ATT was introduced. We also consider individual characteristics that could affect users' privacy concerns as antecedents of privacy concerns in the APCO framework (Smith et al., 2011) to verify that the difference in privacy concerns between the treatment group and control group is due to the ATT. To incorporate these covariates into the DID analysis, we used the DR approach that combines both the outcome regression (OR) and inverse probability weighting (IPW) approaches proposed by Sant'Anna and Zhao (2020).

We considered six individual characteristics: the year of birth (born), gender, digital capabilities related to protecting information privacy (PA), highest education level (Edu), income, and monthly payments of mobile services (Exp) as covariates. Previous studies showed that demographic characteristics are related to privacy concerns (Benamati et al., 2017; Smith et al., 2011). We also considered the digital capabilities related to protecting information privacy as a proxy for privacy literacy that could affect privacy concerns (Rosenthal et al., 2020). Lastly, we considered the monthly payments of mobile services as a proxy for the usage of smartphones and mobile services. We assumed that the usage of mobile services can be related to personal privacy experience which affect privacy concerns (Benemati et al., 2017; Ozdemir et al., 2017). The measurement and statistics of individual characteristics in Korea Media Panel Survey data are summarized in Tables 1 and 2.

Table 1. Description of covariates

Covariates	Measurement
PA	It is measured by five questions using a 5 Likert scale related to the digital capabilities of information privacy protection.
Gender	Male: 1, Female: 2
Birth	The year of birth.
Edu	The highest education level is classified into six levels.
Income	Monthly income is classified into eight levels.
Exp	Monthly payments of mobile services (thousands KRW/month).

Table 2. Summary statistics for covariates

Covariates	Control (non-iOS)	Treatment (iOS)	Diff	p-value
PA	3.2636	4.2390	-0.9754	0.0000
Gender	1.5481	1.6484	-0.1003	0.0586
Birth	1973.6770	1988.8240	-15.1472	0.0000
Edu	4.5051	4.9341	-0.4290	0.0000
Income	4.0128	3.7912	0.2216	0.3307
Exp	60.7065	65.3681	-4.6616	0.0033
N	2,653	91		

Table 3. Questionnaires for privacy concerns

Questionnaire
Q1. I am concerned that personal information I do not remember may have remained online.
Q2. I am concerned that online sites ask for too much personal information when signing up.
Q3. I am generally concerned about my privacy when using the Internet.
Q4. People who do not reveal who they are online are suspicious.
Q5. I am concerned that my personal information, including my photo and name, could be stolen online.

Privacy concerns, the dependent variable of this analysis, are measured by four items with a 5 Likert scale in Korea Media Panel Survey data. The five questions related to privacy concerns are summarized in Table 3.

4. Results

The result of dynamic DID is summarized in Table 4 and the trends of the aggregated treatment effect is described in Figure 2. First, the parallel trend assumption is satisfied after conditioning on observed covariates ($\chi^2(4) = 1.5052$, p-value = 0.8257 for the null hypothesis that all pre-treatments are equal to 0). It means there is no statistical evidence that the privacy concerns between the treatment and control groups were different before the ATT was introduced.

Second, the result of dynamic DID shows that the ATT has a negative impact on the users' privacy concerns in the first year. It is consistent with previous findings that users' privacy concerns can be increased due to the strengthened personal data protection regulation by providing information related to the data collectors' practices related to personal data collection. However, in the second and third years after the introduction of ATT, there has been no statistically significant impact on users' privacy concerns. One possible explanation is that the effect of privacy awareness is dominant in the short term after the introduction of ATT. ATT asks users' explicit consent to allow third-party apps to track their personal data in iOS with a pop-up notice when they use the app for the first time after the ATT took effect by updating iOS. This means that iOS users were newly aware of the prevalence of third-party apps' practices of tracking personal data in iOS at an early stage after the ATT took effect. Thus, the newly awareness about the third-party apps' tracking personal data outweighs the fact that their privacy can be protected by the ATT in the short term. However, the negative effects due to newly awareness seem to be diluted by the positive effect of the ATT on users' privacy perceptions as time goes on. These results also suggest that the effect of the strengthened personal data protection regulation can be misinterpreted if it does not consider the dynamic effect, considering that the average post-treatment effect is not statistically significant.

Third, these results support the proposed approach that using the platform-level privacy regulation as a proxy for privacy regulation at the national level could be a reasonable approach to overcoming the difficulty of setting up the treatment group and control group. Based on dividing iOS users and non-iOS users into treatment and control groups, respectively, and conditioning observed covariates, we found that the parallel trend assumption is satisfied as well as the aggregated treatment effect is statistically significant.

Table 4. The aggregated treatment effect estimates

	Coef	Std. Err.
Pre_avg	0.0013	0.3110
Post_avg	0.0907	0.1034
-4	-0.0914	0.1141
-3	0.1502	0.1099
-2	-0.1112	0.1031
-1	0.0576	0.0948
0	**0.2235**	**0.1251**
1	0.1373	0.1067
2	-0.0889	0.1188

Note. Bold indicates a p-value is less than 0.1.

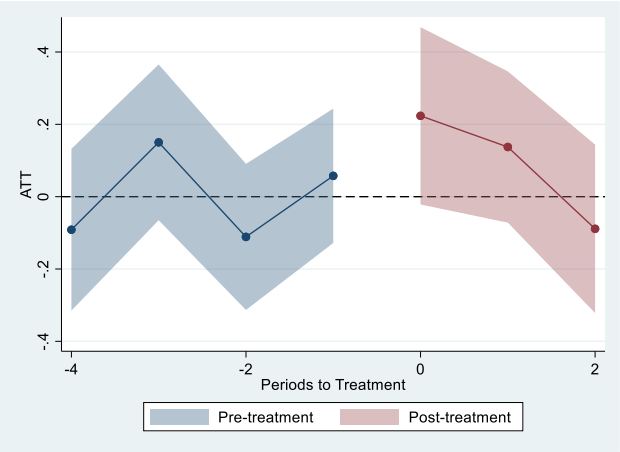

Figure 2. The trends of the aggregated treatment effect

5. Conclusion

This paper investigated the strengthened personal data protection regulations on users' privacy concerns. Considering that smartphone platforms are perceived as privacy regulators in

their platforms, we proposed the approach of using the smartphone platforms' privacy regulations as a proxy for the personal data protection regulation to overcome the difference in setting up treatment and control groups.

We found that the introduction of ATT had a positive impact on iOS users' privacy concerns in the first year; however, there were no significant results in the second and third years after the introduction of ATT. This result is consistent with the previous findings that personal data protection could positively and negatively affect users' privacy concerns by increasing trustworthiness and privacy awareness, respectively. Our distinct contribution point is providing empirical evidence on how the effect of strengthened personal data protection regulation on users' privacy concerns changes over time after the regulation is introduced through dynamic DID analysis. This result also implies that further studies should consider the dynamic effect of personal data protection regulation on users' privacy perceptions.

This paper also provides a policy implication. Regulators need to consider that users' privacy concerns are increased in the short term when the strengthened personal data protection regulation is introduced by increasing users' privacy awareness. It is suggested that regulators devise some measures to ensure trustworthiness at the time of the introduction of regulations to dilute this effect.

References

Bauer, P. C., Gerdon, F., Keusch, F., Kreuter, F., & Vannette, D. (2022). Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. Information, Communication & Society, 25(14), 2101-2121.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly, 1017-1041.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents–Privacy Concerns–Outcomes model. Journal of Information Science, 43(5), 583-600.

Bergmann, M. (2008). Testing privacy awareness. In IFIP Summer School on the Future of Identity in the Information Society (pp. 237-253). Berlin, Heidelberg: Springer Berlin Heidelberg.

Callaway, B., & Sant'Anna, P. H. (2021). Difference-in-differences with multiple time periods. Journal of econometrics, 225(2), 200-230.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. Journal of Computer-Mediated Communication, 21(5), 368-383.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information systems research, 17(1), 61-80.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. Computers in Human Behavior, 121, 106806.

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. Information Technology & People, 35(8), 181-204.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. Journal of management information systems, 24(2), 13-42.

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022, June). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (pp. 508-520).

LaRose, R., & Rifon, N. (2006). Your privacy is assured-of being disturbed: websites with and without privacy seals. New Media & Society,

8(6), 1009-1029.

Nooren, P., Van Gorp, N., van Eijk, N., & Fathaigh, R. Ó. (2018). Should we regulate digital platforms? A new framework for evaluating policy options. Policy & Internet, 10(3), 264-301.

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. European Journal of Information Systems, 26(6), 642-660.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of consumer affairs, 39(2), 339-362.

Rosenthal, S., Wasenden, O. C., Gronnevet, G. A., & Ling, R. (2020). A tripartite model of trust in Facebook: acceptance of information personalization, privacy concern, and privacy literacy. Media Psychology, 23(6), 840-864.

Sant'Anna, P. H., & Zhao, J. (2020). Doubly robust difference-in-differences estimators. Journal of econometrics, 219(1), 101-122.

Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., & Cranor, L. F. (2016, February). Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In NDSS workshop on usable security (Vol. 10).

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 989-1015.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. Research in personnel and human resources management, 8(3), 349-411.

Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. Journal of Interactive Marketing, 56(1), 137-158.

Van Hoboken, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. Computer Law & Security Review, 41, 105557.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(6), 1.

Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. Journal of interactive marketing, 18(1), 53-69.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 28(3), 889-897.