How Communicating about the Privacy Notice Impacts Trust. The Role of Clarity and Transparency

Niccolò Testi[1], **Giacomo Gistri**[2]

Abstract

Considering the widespread use of privacy labels to inform users about apps' privacy practices, this study investigates the impact of privacy notice communication content and its clarity on trust in AI-based health apps. Drawing on Signaling Theory, a 3x1 between-subjects experimental design was used to examine how varying levels of privacy notice communication content completeness — ranging from minimal (data collection) to comprehensive (data collection, processing, dissemination) — influence perceived trust, mediated by perceived clarity and transparency. Results show that a more comprehensive privacy notice communication significantly enhances trust, with clarity and transparency serving as serial mediators. These findings highlight the importance of balancing content detail with design clarity to reduce information asymmetry, fostering trust in privacy-sensitive applications. Practical implications suggest that app developers and policymakers should adopt user-friendly yet informative communication strategies to meet regulatory standards and enhance user confidence.

Keywords: *privacy label, privacy notice communication, trust, transparency, clarity*

Acknowledgment: *this article is the result of the project "Customer Delight: toward a New Conceptualization of the Construct in Technological Environments Powered by Artificial Intelligence" code 2022LHCKAL, CUP D53D23006560006, funded by the PRIN 2022 program co-financed by the European Union - Next Generation EU – PNRR Mission 4 Component 2 Investment 1.1.*

[1] Research Fellow, Department of Political Science, Communication and International Relations, University of Macerata (Italy), n.testi@unimc.it.

[2] Professor of Marketing, Department of Political Science, Communication and International Relations, University of Macerata (Italy), giacomo.gistri@unimc.it.

Introduction

In recent years, there has been a global increase in the adoption and usage of apps that process personal data (Goel & Sahil, 2024). User privacy has become more important in the digital age, focusing on the acquisition, retention, and utilization of personal data, and its utilization by third parties (Nass et al., 2009). Instances of data mishandling by apps have led to a surge in privacy concerns among consumers, who are becoming more aware of the potential risks associated with sharing their personal information with the companies behind these apps (Bandara et al., 2021).

Increasingly, apps are using artificial intelligence (AI) (Carole et al., 2024). As Gerke & Rezaeikhonakdar (2022) noted, AI in mobile health apps is used to identify patterns and make predictions about the user's health. To do so, AI-powered mobile health apps rely on large datasets of highly sensitive mental and physical health data. Thus, the authors warn that these require stronger safeguards than other apps to protect user privacy and prevent misuse.

In response to these growing concerns, regulatory bodies have taken action. The General Data Protection Regulation (GDPR), for instance, mandates that companies provide users with clear and transparent privacy notices detailing their data handling practices (Wolford, 2024), which can help companies build consumer trust (Wu et al., 2012). However, users often struggle to comprehend privacy notices which tend to be lengthy and complex and, consequently, fail to defend themselves from data misuse (Dehling & Sunyaev, 2023; Meier et al., 2020).

Privacy concerns in mobile health apps are especially significant, as many fail to ensure personal data privacy (Hussain et al., 2018). Privacy on mobile health applications necessitates transparency of data practices (Huckvale et al., 2019; Minen et al., 2018; Robillard et al., 2019), which can foster the trust that is necessary for user adoption (LaMonica et al., 2021). Privacy policies are essential to ensure transparency and compliance with privacy regulations to avoid the misuse of the data (Hakiem et al., 2024). However, these apps often fail to provide app privacy notices and, when they do, the privacy policies do not make privacy practices transparent to users because they are complex to understand (Sunyaev et al., 2015).

In an attempt to increase transparency of privacy practices, companies such as Apple and Google have required all app developers to create privacy labels when submitting new apps or app updates (Khandelwal et al., 2023). Privacy labels are a form of non-legally mandatory communications to consumers about the apps' privacy notices, aimed at simplifying and clarifying the apps' privacy practices (Li et al., 2022).

Communications of this kind might have a positive impact on consumer trust. Vail et al., (2008) suggest that providing clear and concise communications regarding companies' privacy policies can enhance consumers' perception of fair treatment by the organization while ensuring compliance with relevant legal requirements. Indeed, privacy policy clarity is beneficial to companies because consumers highlight that consumers are often deterred from engaging with websites or completing transactions when privacy policies are unclear, which makes consumers uncertain about how their information will be used (Milne et al., 2004). Brunotte et al. (2023) found that the majority of users are interested in receiving explanations about companies' privacy practices and that these explanations can be important steps toward increasing trust.

However, while the potential contribution of providing clear privacy policies has been addressed by researchers, it is not clear what is the most effective way to create clear communications about privacy policies (Gluck et al., 2016; McDonald et al., 2009) to maximize their effectiveness in terms of increased transparency and trust. This gap between the need for transparency and the ability to convey information effectively remains a challenge.

Drawing from the concept of information asymmetry (Akerlof, 1970) and Signalling Theory (Spence, 1973) as a framework for understanding the effect of privacy communications as signals provided by companies to increase transparency by reducing information asymmetry (Connelly et al., 2011), this study compares the effects of three distinct privacy communications on trust towards the brand. We developed the content of these communications, referring to it as "Privacy Notice Communication Content" (PNCC). The content was divided into three sections, each paraphrasing one of the key parts typically found in privacy notices, as outlined by Eggers et al. (2023): the first addressed the app's privacy practices related to data collection, the second focused on data processing, and the third covered data dissemination. Results show how the reduction of information in such communication may hurt the trust in the brand and this effect is serially mediated by the perception of clarity and transparency. These findings provide valuable insights for app developers, policymakers, and regulators.

Theoretical Background and Research Objectives

When relevant information in an economic relationship is not provided or is provided in an unclear way, information asymmetry occurs between the party that possesses more or better information and the other (Akerlof, 1970). Reducing information asymmetry is crucial for increasing trust (Akerlof, 1970). Trust is a belief in another's reliability and occurs when one party (the trustor) becomes vulnerable to another (the trustee), expecting the trustee to act in the trustor's best interest (Schilke et al., 2021). For companies, earning consumers' trust is important: not only trust make the initiation of transactions possible (Akerlof, 1970), but is also a key variable in building and maintaining customer loyalty (Morgan & Hunt, 1994). Receiving complete information significantly increases information transparency, which boosts trust in the information provider (Kanagaretnam et al., 2010).

In corporate marketing, information must meet criteria such as clarity to be considered transparent (Leitch, 2017). Indeed, clarity of communications is required to make them more transparent (Luzak et al., 2023). Clarity refers to the extent to which consumers perceive brand messages to be understandable and reflects the information perspective that views transparency as the extent of information asymmetry reduction (Montecchi et al., 2024).

Signaling Theory (Spence, 1973) provides insight into how the more informed party can reduce information asymmetry by sending information as signals that convey its underlying qualities to the less informed party, such as being trustworthy (Connelly et al., 2011).

One type of signal companies can use to indicate their trustworthiness is the provision of privacy notices, which act as "regulatory compliance signals" indicating adherence to legal requirements (Mavlanova et al., 2012), such as those outlined by the GDPR. These signals aim to mitigate information asymmetry and enhance trust in the company by informing users about the company's data privacy practices regarding customers' data (Mavlanova et al., 2016).

Communications by companies that provide information about their data privacy practices can be considered "transparency enhancing tools" (TETs) that provide the users with necessary information on how their data have been stored, exchanged, processed, and used (Hansen, 2008; Janic et al., 2013). These are aimed at increasing awareness and reducing information asymmetry about a company's privacy policy (Zimmermann, 2015).

For this study, we created a Privacy Notice Communication (PNC) as a TET meant to increase the clarity of the app privacy policy and perceived app transparency. The PNC content (PNCC) includes the three key aspects of a firm's privacy practices: personal data collection, data processing (storage and protection), and data dissemination (use and

sharing) (Eggers et al., 2023; Kelley et al., 2009). The division into three parts allows us to manipulate the amount of information given to the participants in the PNC: we can give the complete PNCC including data collection, processing, and dissemination, or a partial PNCC including data collection and processing or data collection only.

Since providing more rather than less information reduces information asymmetry (Akerlof, 1970), increasing information transparency and trust in the information provider (Kanagaretnam et al., 2010), we expect that:

H1: Increasing the amount of information provided in the PNCC leads to higher Trust in the Brand.

Further, considering that reducing information asymmetry can make brand messages be perceived as more clear (Montecchi et al., 2024) and that information clarity positively influences transparency (Luzak et al., 2023), we hypothesize that:

H2: Privacy Policy Clarity and perceived App Transparency serially mediate the relationship between the PNCC and Trust in the Brand. Specifically, decreasing the amount of information provided in the PNCC decreases perceived Privacy Policy Clarity, which in turn decreases perceived App Transparency, which in turn reduces Trust in the Brand.

Methodology

The 3x1 between-subjects experimental design was chosen to isolate and compare the effects of varying levels of privacy notice communication content (PNCC) on perceived trust, clarity, and transparency. This approach allowed for clear manipulation of the independent variable (PNCC completeness) across three conditions—complete (data collection, processing, dissemination), moderate (data collection and processing), and minimal (data collection only). By randomly assigning participants to one of these groups, the design ensured control over extraneous variables while maintaining ecological validity in evaluating privacy communications for AI-based health apps.

We measured perceived Trust toward the Brand (4 items, Likert 1-5; α=0,81) (Chaudhuri & Holbrook, 2001), the perceived Clarity of the Privacy Policy (3 items, Likert 1-5, α=0.9) (Bart et al., 2005), and the perceived App Transparency (3 items, Likert 1-5; α=0,87). The measures of trust, clarity, and transparency were chosen for their theoretical and practical relevance. Trust is a critical outcome variable, as it reflects consumer confidence in the brand and significantly influences app adoption and loyalty (Schilke et al., 2021). Clarity and transparency were included as mediators based on their central role in Signaling Theory and privacy research, which emphasize the importance of clear and transparent communications in reducing information asymmetry (Connelly et al., 2011). These constructs were operationalized using validated scales, ensuring reliability and relevance to the research objectives.

The independent variable, PNCC, was a categorical variable with three levels: (I) information on data collection, data processing, and data dissemination; (II) information on data collection, and processing; (III) information on data collection.

The study involved a hypothetical AI-based health app scenario, with 180 Italian respondents recruited via Prolific (mean age 34.31, 41.6% female) randomly assigned to one out of three experimental groups. Prolific is a widely accepted platform for behavioral research, known for its diverse and high-quality participant pools. Random assignment was employed to distribute participants evenly across conditions, ensuring internal validity. The sample comprised Italian adults who reflected a typical demographic profile for app users. This approach aligns with established research practices in experimental studies on consumer behavior.

The sample size of 180 participants (60 per condition) was determined based on a power analysis to detect medium effect sizes (f=0.25) with a statistical power of 0.80 and an alpha level of 0.05 for ANOVA. This ensured the ability to detect significant differences between groups. The sample size is appropriate for the research context, as it balances practical constraints with statistical rigor, providing reliable and generalizable insights into the impact of privacy communications.

The questionnaire was created through SurveyMonkey. Stimuli were based on the guidelines by Luzak et al. (2023). We asked also for the collaboration of a privacy expert team to verify that the PNCC conveyed all relevant information clearly, avoiding legal jargon. Stimuli are available upon request.

Results

To test our H1, we ran a one-way ANOVA. The homogeneity of variances was assessed using Levene's test [$F(2,177) = 0.31$, $p = .97$]. There was a significant main effect of the PNCC on the users' perceived Trust in the Brand, $F(2, 177) = 8.278$, $p < 0.001$, $\eta^2=0.09$ indicating a medium effect size. Post hoc test revealed that users perceived a higher Trust in the Brand if the PNCC is complete, i.e., it reports information on data collection + processing + dissemination (3.29) compared to the partial PNCC reporting data collection + processing (2.96) or only data collection (2.60). This leads to confirm H1.

(I) PNCC	(J) PNCC	Mean Difference (I-J)	SE	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
data collection + processing + dissemination	data collection + processing	.333	.167	.048	.002	.664
	data collection	.689	.169	.000	.355	1.024
data collection + processing	data collection + processing + dissemination	-.333	.167	.048	-.664	-.002
	data collection	.356	.165	.033	.029	.682
data collection	data collection + processing + dissemination	-.689	.169	.000	-1.02	-.355
	data collection + processing	-.356	.165	.033	-.682	-.029

Table 1. Post hoc test

To verify H2, we tested a serial mediation model using the SPSS Process macro by Hayes (2022). We chose the bootstrap confidence interval (CI) approach to mediation and ran Model 6 with 5,000 bootstrapping samples.

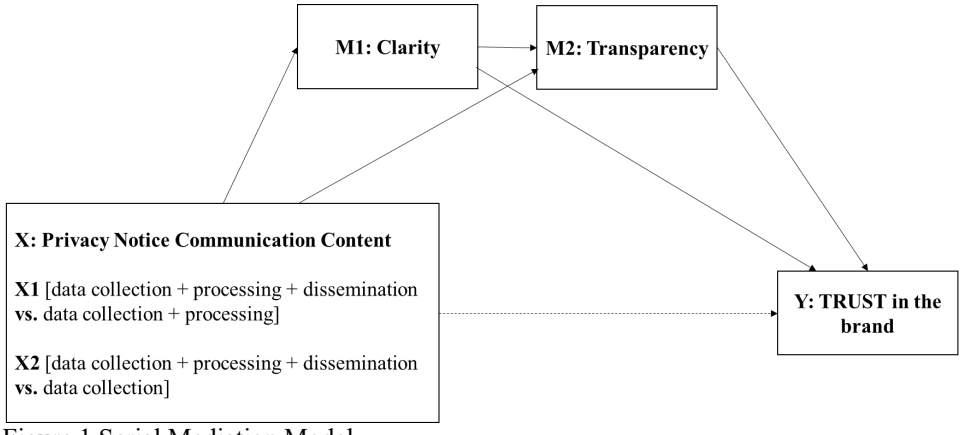

Figure 1 Serial Mediation Model

	M_1 (Clarity)			M_2 (Transparency)			Y (Trust in the Brand)		
Antecedent	Coeff.	*SE*	*p*	Coeff.	*SE*	*p*	Coeff.	*SE*	*p*
X_1	-.352	.171	*<.05*	-.248	.139	*NS*	-.014	.123	*NS*
X_2	-.709	.173	*<.001*	-.389	.146	*<.05*	-.101	.130	*NS*
M_1 (Clarity)	---	---	---	.554	.061	*<.001*	.291	.064	*<.001*
M_2 (Transparency)	---	---	---	---	---	---	.488	.066	*<.001*
Constant	3.748	.124	*<.001*	1.467	.0248	*<.001*	.473	.237	*<.05*
	R^2=0.08			R^2=0.39			R^2=0.53		
	F(2,177)=8.412;p<.001			F(3,176)=38.249;p<.001			F(4,175)=49.919;p<0.001		

Indirect Effects of X on Y	**Effect**	**Boot SE**	**Boot 95% CI**	
PNCC=>CLARITY=>TRUST				
X_1	-.102	.059	-.234	-.002
X_2	-.206	.076	-.373	-.077
PNCC=>TRANSPARENCY=>TRUST				
X_1	-.121	.065	-.258	-.003
X_2	-.190	.077	-.338	-.040
PNCC=>CLARITY=>TRANSPARENCY=>TRUST				
X_1	-.095	.050	-.201	-.002
X_2	-.192	.065	-.338	-.083

Table 2 Serial Mediation Analisis

Results show how, in the context of the App used to monitor personal health, communication about the privacy notice presenting partial information, reduces the Trust in the brand compared to more complete information. Specifically, decreasing the information provided in the PNCC negatively affects the perceived clarity, which in turn decreases the perceived Transparency, which in turn reduces the Trust in the brand. This leads to confirm H2.

Discussion, Implications, and Future Development

The findings of this study give insights into the importance of comprehensive PNCC in building trust toward the brand that handles personal data and employs AI. Specifically, by reducing the amount of information communicated in the privacy labels, the trust in the brand decreases. Such an effect is due to the reduction of the perceived clarity of the communication that, in turn, reduces the perceived transparency, which decreases trust.

This study has theoretical implications for the further validation of the use of Signaling Theory in marketing research, as it demonstrates how detailed privacy communications act as trust-enhancing signals, highlighting the interplay between clarity, transparency, and trust. On one hand, the study builds on the work of Mavlanova et al. (2012, 2016) who consider privacy communications informing users about a company's privacy practices as a way for the company to signal its trustworthiness. On the other, it suggests that privacy labels are not mere informational tools but TETs that shape consumer perceptions and attitudes, supporting the assertions by Hansen (2008) and Janic et al. (2013) about the role of privacy communications as TETs.

The significant impact of transparency on trust aligns with findings by Kanagaretnam et al. (2010) on the positive relationship between transparency and trust. The study reveals that partial information, especially when limited to data collection only, can significantly

undermine trust through reduced clarity and transparency. This finding provides insights for app developers, who should avoid overly reducing information in privacy communications, as clarity and transparency are drivers of trust.

Finally, policymakers and regulators can draw from these findings to define guidelines for privacy notices and related privacy communications. Since incomplete disclosures of privacy practices hurt clarity and transparency, it may be useful to mandate a baseline level of informational detail.

Limitations of this study include the use of a hypothetical app and a sample geographically limited to one Country. To address these limitations, future developments should test such effects using field studies and explore cross-cultural perspectives.

References

Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488. https://doi.org/10.2307/1879431

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/EJM-06-2019-0515

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing*, *69*(4), 133–152. https://doi.org/10.1509/jmkg.2005.69.4.133

Brunotte, W., Specht, A., Chazette, L., & Schneider, K. (2023). Privacy explanations – A means to end-user trust. *Journal of Systems and Software*, *195*, 111545. https://doi.org/10.1016/j.jss.2022.111545

Carole, K. S., Theodore Armand, T. P., & Kim, H. C. (2024). Enhanced Experiences: Benefits of AI-Powered Recommendation Systems. *2024 26th International Conference on Advanced Communications Technology (ICACT)*, 216–220. https://doi.org/10.23919/ICACT60172.2024.10471918

Chaudhuri, A., & Holbrook, M. B. (2001). The Chain of Effects from Brand Trust and Brand Affect to Brand Performance: The Role of Brand Loyalty. *Journal of Marketing*, *65*(2), 81–93. https://doi.org/10.1509/jmkg.65.2.81.18255

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Dehling, T., & Sunyaev, A. (2023). A Design Theory for Transparency of Information Privacy Practices. *Information Systems Research*, isre.2019.0239. https://doi.org/10.1287/isre.2019.0239

Eggers, F., Beke, F. T., Verhoef, P. C., & Wieringa, J. E. (2023). The Market for Privacy: Understanding How Consumers Trade Off Privacy Practices. *Journal of Interactive Marketing*, *58*(4), 341–360. https://doi.org/10.1177/10949968221140061

Gerke, S., & Rezaeikhonakdar, D. (2022). Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps. *Intelligence-Based Medicine*, *6*, 100061. https://doi.org/10.1016/j.ibmed.2022.100061

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 321–340. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck

Goel, A., & Sahil, G. (2024). Growth of mobile applications and the rise of privacy issues. *International Journal of Electronic Finance*, *13*(1), 20–35. https://doi.org/10.1504/IJEF.2024.135162

Hakiem, N., Afrizal, S. H., Setiadi, Y., Hadid, S. A., Riasetiawan, M., & Zulhuda, S. (2024). Security and Privacy Policy Assessment in Mobile Health Applications: A Literature Review. *Journal of System and Management Sciences*, *14*(2). https://doi.org/10.33168/JSMS.2024.0222

Hansen, M. (2008). Marrying Transparency Tools with User-Controlled Identity Management. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato, & L. Martucci (Eds.), *The Future of Identity in the Information Society* (pp. 199–220). Springer US. https://doi.org/10.1007/978-0-387-79026-8_14

Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (Third edition). The Guilford Press.

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Network Open*, *2*(4), e192542. https://doi.org/10.1001/jamanetworkopen.2019.2542

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on Android platform. *Telematics and Informatics*, *35*(5), 1335–1354. https://doi.org/10.1016/j.tele.2018.03.005

Janic, M., Wijbenga, J. P., & Veugen, T. (2013). Transparency Enhancing Tools (TETs): An Overview. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 18–25. https://doi.org/10.1109/STAST.2013.11

Kanagaretnam, K., Mestelman, S., Nainar, S. M. K., & Shehata, M. (2010). Trust and reciprocity with transparency and repeated interactions. *Journal of Business Research*, *63*(3), 241–247. https://doi.org/10.1016/j.jbusres.2009.03.007

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A 'nutrition label' for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1–12. https://doi.org/10.1145/1572532.1572538

Khandelwal, R., Nayak, A., Chung, P., & Fawaz, K. (2023). *The Overview of Privacy Labels and their Compatibility with Privacy Policies* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2303.08213

LaMonica, H. M., Roberts, A. E., Lee, G. Y., Davenport, T. A., & Hickie, I. B. (2021). Privacy Practices of Health Information Technologies: Privacy Policy Risk Assessment Study and Proposed Guidelines. *Journal of Medical Internet Research*, *23*(9), e26317. https://doi.org/10.2196/26317

Leitch, S. R. (2017). The transparency construct in corporate marketing. *European Journal of Marketing*, *51*(9/10), 1503–1509. https://doi.org/10.1108/EJM-07-2017-0456

Li, Y., Chen, D., Li, T., Agarwal, Y., Cranor, L. F., & Hong, J. I. (2022). Understanding iOS Privacy Nutrition Labels: An Exploratory Large-Scale Analysis of App Store Data. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–7. https://doi.org/10.1145/3491101.3519739

Luzak, J., Wulf, A. J., Seizov, O., Loos, M. B. M., & Junuzović, M. (2023). ABC of Online Consumer Disclosure Duties: Improving Transparency and Legal Certainty in Europe. *Journal of Consumer Policy*, *46*(3), 307–333. https://doi.org/10.1007/s10603-023-09543-w

Mavlanova, T., Benbunan-Fich, R., & Koufaris, M. (2012). Signaling theory and information asymmetry in online commerce. *Information & Management*, *49*(5), 240–247. https://doi.org/10.1016/j.im.2012.05.004

Mavlanova, T., Benbunan-Fich, R., & Lang, G. (2016). The role of external and internal signals in E-commerce. *Decision Support Systems*, *87*, 59–68. https://doi.org/10.1016/j.dss.2016.04.009

McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009). A Comparative Study of Online Privacy Policies and Formats. In I. Goldberg & M. J. Atallah (Eds.), *Privacy Enhancing Technologies* (Vol. 5672, pp. 37–55). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03168-7_3

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making. *Media and Communication*, *8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846

Minen, M. T., Stieglitz, E. J., Sciortino, R., & Torous, J. (2018). Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. *Headache: The Journal of Head and Face Pain*, *58*(7), 1014–1027. https://doi.org/10.1111/head.13341

Montecchi, M., Plangger, K., West, D., & De Ruyter, K. (2024). Perceived brand transparency: A conceptualization and measurement scale. *Psychology & Marketing*, mar.22048. https://doi.org/10.1002/mar.22048

Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, *58*(3), 20–38. https://doi.org/10.1177/002224299405800302

Nass, S. J., Levit, L. A., & Gostin, L. O. (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (p. 12458). National Academies Press. https://doi.org/10.17226/12458

Robillard, J. M., Feng, T. L., Sporn, A. B., Lai, J.-A., Lo, C., Ta, M., & Nadler, R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*, *17*, 100243. https://doi.org/10.1016/j.invent.2019.100243

Schilke, O., Reimann, M., & Cook, K. S. (2021). Trust in Social Relations. *Annual Review of Sociology*, *47*(1), 239–259. https://doi.org/10.1146/annurev-soc-082120-082850

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, *87*(3), 355. https://doi.org/10.2307/1882010

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, *22*(e1), e28–e33. https://doi.org/10.1136/amiajnl-2013-002605

Vail, M. W., Earp, J. B., & AntÓn, A. I. (2008). An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. *IEEE Transactions on Engineering Management*, *55*(3), 442–454. https://doi.org/10.1109/TEM.2008.922634

Wolford, B. (2024). *Writing a GDPR-compliant privacy notice (template included)*. Retrieved from https://gdpr.eu/privacy-notice/. (Last accessed: April 30, 2024)

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. https://doi.org/10.1016/j.chb.2011.12.008

Zimmermann, C. (2015). *A Categorization of Transparency-Enhancing Technologies* (No. arXiv:1507.04914). arXiv. http://arxiv.org/abs/1507.04914