

Privacy Policies and the use of Personal Data as Strategic Variables for Entrepreneurs in the Health Apps Market

Cláudia Cardoso¹, Cândida Sofia Machado¹ and Natália Lemos³

¹Applied Management Research Unit (UNIAG), School of Management, Polytechnic University of Cávado and Ave (IPCA), Barcelos, Portugal

²2Ai – Applied Artificial Intelligence Laboratory, School of Technology, Polytechnic University of Cávado and Ave (IPCA), Barcelos, Portugal

ccardoso@ipca.pt

cmachado@ipca.pt

nslemos@ipca.pt

Abstract: Background: Health apps cover many areas and functions and are easily available. However, massive use of personal data has security and privacy risks. Although there is the widespread idea that privacy is important for app users, their efforts to protect their personal data are usually low or none. Evidence from online services show that privacy protection is still an issue, and many app developers fail on the disclosure of a privacy policy, even if it is mandatory. This is evident for health apps also, despite the sensitivity of personal health data. Entrepreneurs must choose an adequate monetization model for their health app business, including privacy concerns. Objectives: We intend to explain how the availability of the privacy policy of a health app and how the decision of an app to explicitly inform users on the use of personal data for micro-segmentation relates with diverse revenue sources, treating those variables as business strategic variables. Methods: We performed a cross-sectional study of health apps available in Portugal. We use logit and probit regression models to establish cause-effect relations between variables. Results: If a health app is downloaded for free or if it includes in-app purchases, it will be more probable to have a privacy policy and to explicitly inform users on the use of personal data. However, the inclusion of ads within the app is not relevant. We conclude that the disclosure of privacy policies and the use of personal data cannot be disconnected from the business model of the app.

Keywords: Privacy Policy, Micro-segmentation, Personal Data, Health Apps, Monetization Models

1. Introduction

Information technologies are seen as powerful tools to help overcome the challenges posed to health systems. Nowadays, health apps cover many areas and functions and are easily available. However, the massive use of information, especially personal data, has security and privacy risks. Regulators try to overcome those risks by preparing rules to ensure that privacy policies are disclosed, and consumers know and agree with the use of their personal data.

In this paper, we intend to explain how the availability of the privacy policy of an app relates with other revenue sources, treating the disclosure of the privacy policy as a business strategic variable. Also, we intend to explain why users are or are not explicitly informed of the use of personal data for micro-segmentation. To achieve this, first we present and describe data; and, secondly, we perform regression analysis.

We contribute to the existing literature not only by studying the behavior of apps on privacy policy disclosure and use of personal data practices but also by explaining the absence of a privacy policy or the lack of accuracy and transparency regarding the provision of information on the use of personal data as a conscious decision taken to conceal the business model of the app. And this should concern developers, users, and regulators in a sector where personal data is particularly sensitive.

2. Theoretical Framework

Although there is the widespread idea that the privacy of personal data is important for app users, the efforts they make to protect their personal data are usually low and often none. This is the so called “privacy paradox”: what online users think about privacy protection is not what they do to protect privacy, in fact. Another piece of evidence is that online users can disclose personal data if, in return, they can benefit from it. This is the so called “privacy calculus”, that Zhu et al. (2021) showed that is presented in mHealth apps.

Empirical analysis shows contradictory results on how consumers respond to data and privacy protection. Aydin and Silahtaroglu (2021) found that mentioning the privacy policy in the description of the app is important to explain higher scores from users but not to explain downloads of the app. In a previous study, on three European countries, only in the Netherlands data protection increased the willingness to pay for the health app. But, in all

three countries, data protection increased the likelihood of downloading the app (Lupiáñez-Villanueva et al., 2020).

The disclosure of privacy policies is mandatory whenever companies collect, manage, and use personal information from users. Nonetheless, evidence from online services, and specifically from apps, show that privacy protection is still an issue, and many app developers fail on the disclosure of a privacy policy. Moreover, even when the privacy policy is disclosed, many times it does not comply with regulation, or it is not suited to the functions of the app itself. This is a reality common to all categories of apps (Alamri et al., 2022; Story et al., 2018), and health apps are no exception. Sunyaev et al. (2015) showed that only 30.5% of 600 mHealth apps have a privacy policy. Papageorgiou et al. (2018) showed that 15% of 20 free health apps, with at least 100,000 downloads, in 2016, did not have a privacy policy available. O'Loughlin et al. (2019) indicated that only 49% of 116 apps, searched using the term “depression”, disclose the privacy policy. The study of Fan et al. (2020) reveals that 23.7% of 796 health apps do not provide a complete privacy policy. Alfawzan et al. (2022) showed that, of the 23 of the most popular women's mHealth apps, 16 (70%) have a privacy policy. The study of Iwaya et al. (2023) revealed significant privacy and security of personal data issues, for mental health apps, aggravated by the sharing of data with third parties, such as advertisers.

Despite the variety of figures, studies showed that there is a significant number of health apps in all samples with no privacy policy available. Evidence corroborates that there is an issue on privacy policies availability, in health apps. The next step is to understand how app developers make the decision to disclose or not a privacy policy and how they decide how accurate the privacy policy should be.

In fact, the use of personal data is a business strategic variable that cannot be dissociated from other business variables, but it is not clear if users see it that way. Tang et al. (2022) conducted a study with users of mobile apps to investigate how user-visible aspects of the app impact perceptions of privacy threat. They concluded that users interpret the presence of advertising as a signal that an app poses a privacy threat (users believe that apps with ads tend to collect more data and are less trustworthy). They also tested if users perceived differences between free apps and paid apps concerning privacy threats, and they concluded that payment for download has not a significant effect. Users seem to see advertising as a signal of data collection, but they do not see payment for download as a way to buy privacy.

The use of personal data can be an important part of a monetization model of an app. In fact, for many apps, the price charged for download (if any) is not the main source of revenue. Apps can also get revenue from advertisement and/or in-app purchases. When combining ads and in-app purchases with the collection and use of personal data for micro-segmentation, the revenues are potentiated, and personal data becomes a relevant economic input. Personal data can additionally be sold to third parties, either for micro-segmentation or for other purposes (Cecere et al., 2022; Polykalas and Prezerakos, 2019). However, contrary to the other sources of revenue, collecting and sharing data for revenue is only perceived by users if it is explicitly presented, and the proper way to communicate the use of personal data is in a privacy policy.

3. Data and Methodology

3.1 Sample

We performed a cross-sectional study of health apps available in Portugal. For this study, a sample of health apps was collected on July 11, 2021. The inclusion criteria were mobile apps for Android or iOS systems, available on Google Play Store or Apple App Store platforms, in Portugal, and listed in the Top Free and Top Paid rankings, for categories 'Health & Fitness' and 'Medical Care/Medicine'.

The initial sample of health apps resulted in a set of 2133 apps, some of which were disregarded based on the following exclusion criteria: apps focused on Coronavirus 2019 (COVID-19), given that these are the consequence of an exceptional context; apps with an approach focused solely on exercise or well-being, such as training apps, yoga, meditation, relaxing melodies, among others, since these do not fall within the meaning of mHealth; and apps that are a mere tool to support other activity (and not a service/product by itself).

Following the application of the above criteria, the final sample of the study comprises 1121 health apps from the two major platforms operating in Portugal: Apple App Store and Google Play Store. The variables collected in the dataset are presented in table 1.

Table 1: Variables description

Variables	Description
Dependent variables	
<i>privacy</i>	Dummy variable that specifies if the privacy policy is available (if not = 0; if so = 1)
<i>inform</i>	Dummy variable that specifies if users are explicitly informed about the use of personal data for micro-segmentation purposes (if not = 0; if so = 1)
Independent Variables	
<i>type</i>	Dummy variable that identifies the typology of the app (Free = 0; Paid = 1)
<i>iap</i>	Dummy variable that specifies whether the app has in-app purchases options (if not = 0; if so = 1)
<i>ads</i>	Dummy variable that specifies whether the app has ads (if not = 0; if so = 1)
<i>remuneration</i>	Dummy variable that identifies if the app remunerates the users (if not = 0; if so = 1)
<i>platform</i>	Dummy variable that identifies the platform where the app is marketed (Google Play Store = 0; Apple App Store = 1)
<i>category</i>	Dummy variable that specifies the category in which the app is classified ("Health and Fitness" = 0; "Medical Care/Medicine" = 1)

3.2 Statistical Analysis

Table 2 presents a statistical description of the dataset. Concerning the disclosure of privacy policies, table 2 presents two sub-samples: the sub-sample of apps without privacy policy available (*privacy*=0) and the sub-sample of apps with privacy policy available (*privacy*=1), that is, where users know, before download, how their personal data will be used by the app, and they can make an informed choice about the implications of using that app. On the full sample, 71.63% of the health apps disclose their privacy policy. Additionally, table 2 presents another two sub-samples: the sub-sample of apps that explicitly inform users about the use of personal data for micro-segmentation (*inform*=1) and the sub-sample of apps that do not explicitly disclose that information (*inform*=0).

The variable *inform* is zero for all the apps without privacy policy. However, the most surprising result is that even when apps disclose the privacy policy, only 68.00% of those explicitly inform about the use of personal data for micro-segmentation.

Our sample has 64.94% of health apps classified as "Medical Care/Medicine" and the remaining 35.06% are apps of "Health and Fitness" (variable *category*). The sub-sample of apps without privacy policy and the sub-sample of apps that "do not inform" have higher percentages of "Medical Care/Medicine" apps.

The health apps are available on the two major platforms operating in Portugal: 40.95% on Apple App Store and 59.05% on Google Play Store. The distribution is similar on the sub-samples.

We consider three alternative sources of revenue: (1) to charge or not a price for download (*type*); (2) to have in-app purchases available on the app (*iap*); or (3) to advertise in the app (*ads*). The most common source of revenue is the price of download (38.54% of the health apps are paid). However, regarding the sub-samples in table 2, there are major differences. For apps without privacy policy, there is a higher percentage of paid apps than that of the full sample. For apps with privacy policy, only 33.13% are paid. Also, for apps that "inform users" only 29.30% are paid.

The second source of revenue is the possibility of in-app purchases (20.79% of all apps). Regarding the sub-samples, the percentage of apps with in-app purchases on the group of apps without privacy policy available is less than half than in the other group, and the difference is even bigger between the sub-sample of apps that "inform" and apps that "do not inform".

The third source of revenue is including advertisements. We have 18.29% of apps with in-app ads, and the prevalence is similar between sub-samples.

Finally, we have only 1.16% of apps that remunerate the users of the app. Our data does not have information on the reasons for remunerating users. It can be done to guarantee a significative number of users and/or their engagement (that may guarantee advertising revenues) or to pay for personal data.

Table 2: Descriptive statistics.

Variables	Full sample (N=1121)	Privacy Policy		Information about the use of personal data for micro-segmentation	
		No (N=318)	Yes (N=803)	No (N=575)	Yes (N=546)
<i>privacy</i> = 1	71.63%	-----	-----	44.70%	100.00%
<i>inform</i> = 1	48.71%	0.00%	68.00%	-----	-----
<i>type</i> = 1	38.54%	52.20%	33.13%	47.30%	29.30%
<i>iap</i> = 1	20.79%	11.64%	24.41%	12.70%	29.30%
<i>ads</i> = 1	18.29%	15.41%	19.43%	15.48%	21.25%
<i>remuneration</i> = 1	1.16%	0.31%	1.49%	0.17%	2.20%
<i>platform</i> = 1	40.95%	41.19%	40.85%	41.73%	40.11%
<i>category</i> = 1	64.94%	72.33%	62.02%	68.17%	61.54%

Finally, we have only 1.16% of apps that remunerate the users of the app. Our data does not have information on the reasons for remunerating users. It can be done to guarantee a significative number of users and/or their engagement (that may guarantee advertising revenues) or to pay for personal data.

3.3 Regression Analysis

We analyze the factors that influence the likelihood of disclosure of privacy policy and the likelihood to inform about the use of personal data for micro-segmentation. According to Gujarati and Porter (2011), both the dependent variables *privacy* and *inform* qualify as qualitative dummy variables and, therefore, qualitative response regression models are applied. Qualitative response regression models, or probability models, aim to find the probability p of something happening. The logit model and the probit model are widely used probability models, in econometrics, because they ensure that the probability is between 0 and 1 and that the relationship between the dependent variable and the independent variable is not linear, that is, the probability does not vary linearly with the explanatory factor (Gujarati and Porter, 2011).

Both models are quite similar, and their results are easily comparable. The selection of the most appropriate model is based on the criterion of the highest log likelihood or, in the specific case of this research, on the smallest log likelihood in absolute terms, since we are facing models with negative values of log likelihood (Cameron and Trivedi, 2008).

4. Results and Discussion

4.1 Dependent Variable Privacy

Results for the dependent variable *privacy* are presented in table 3. Results are similar on both regression models. However, considering the log likelihood value of the logit and probit models, table 3 shows that the most appropriate probability model is the probit, whose log likelihood is -638.2008, that is, the highest value.

First, *category* is a statistically significant variable. Being in the “Medical Care/Medicine” category decreases the probability of having privacy policy available by 7.4 percentage points. This result is in line with Alamri et al. (2022). Although, previous studies could not prove the effect of those categories on the disclosure of privacy policies (Story et al., 2018; Sunyaev et al., 2015). Indeed, there are some doubts about the accuracy of the classification within categories that have such close subjects, and a content analysis may be necessary to link the contents of the apps with the probability of having a privacy policy. To this study, this variable is mainly important as a control variable.

The choice of platform to market the app, that is Google Play Store or Apple App Store, does not have a significant effect on the probability of having a privacy policy available. The irrelevance of the platform to explain the disclosure of privacy policies is consistent with previous evidence if we cross results of Alamri et al. (2022), for Apple App Store, and Zimmeck et al. (2019), for Google Play Store. Both studies show similar proportions between apps with or without privacy policy.

Table 3: Estimation results – coefficients and marginal effects (dependent variable privacy)

Variables	Probit Model		Logit Model	
	Coefficients (Standard Errors)	Marginal Effects (Standard Errors)	Coefficients (Standard Errors)	Marginal Effects (Standard Errors)
<i>Category</i>	-0.2276 ** (0.0880)	-0.0740 *** (0.0279)	-0.3784 ** (0.1492)	-0.0726 *** (0.0277)
<i>Platform</i>	0.0967 (0.0881)	0.0320 (0.0290)	0.1547 (0.1473)	0.0303 (0.0287)
<i>Type</i>	-0.4480 *** (0.0915)	-0.1526 *** (0.0316)	-0.7431 *** (0.1535)	-0.1514 *** (0.0318)
<i>Ads</i>	-0.1605 (0.1225)	-0.0549 (0.043)	-0.2685 (0.2086)	-0.0550 (0.0442)
<i>Iap</i>	0.4284 *** (0.1146)	0.1306 *** (0.0314)	0.7456 *** (0.2029)	0.1317 *** (0.0312)
<i>Remuneration</i>	0.5895 (0.5291)	0.1576 (0.1051)	1.0697 (1.0509)	0.1588 (0.1070)
<i>Constant</i>	0.8179 *** (0.0942)		1.3428 *** (0.1612)	
Log likelihood	-638.2008		-638.2676	
LR Chi ² (6)	60.67 ***		60.57 ***	

Note: N = 1121; ** Significant with p-value <0.05; *** Significant with p-value <0.01

We consider three alternative sources of revenue (charge a price, advertise, and have in-app purchases) and a fourth business strategy (remunerate the users). We have two of those variables significant to explain the disclosure of privacy policy.

An app being paid decreases the probability of having a privacy policy available by 15.26 percentage points. We may argue that paid apps' business model does not involve the use, collection and share of substantial personal data and, therefore, the lesser care with the availability of a privacy policy. However, there is ambiguous evidence that paid apps harvest less data than free apps (Han et al., 2019; Kollnig, 2021; Laperdrix et al., 2022).

The presence of ads and the possibility of in-app purchases are two sources of revenue that can be potentiated by customization, using personal data. Therefore, the focus on the use of personal data and its security and privacy issues should be higher. However, the variables *ads* and *iap* have different impact on our dependent variable. On one side, having ads does not significantly influence the availability of privacy policies; while on the other side, having in-app purchases increases the probability of having privacy policy available by 13.06 percentage points. This result is in accordance with Kollnig (2021), that showed that apps, relying on in-app purchases as a revenue source, harvest personal data and, therefore, may be more aware of the need of a privacy policy to maintain user's confidence. Story, et al. (2018) showed that more than 65% of apps with in-app purchases have a link to its privacy policy; and that was the interactive element that contributed more to have a privacy policy available.

Finally, to remunerate users has a positive but not statistically significant effect on the availability of privacy policy. The positive signal is expected since apps mainly remunerate users for their personal data and, thus, privacy and security aspects should be taken care. The absence of statistical significance is, probably, due to the small number of apps on our sample remunerating users (13 from 1121 apps). In fact, despite the use of personal data as a monetization way for many apps, many app developers do not feel the need to pay for data because they can get that data for free, either because of the lack of regulation or supervision, or the lack of control by users.

4.2 Dependent Variable Inform

As for the dependent variable *inform*, estimation results are exhibited in table 4. Results are similar for both regression models, but we will analyze the results of the probit model, whose log likelihood is -734.83821, that is, the highest value.

Table 4: Estimation results – coefficients and marginal effects (dependent variable inform)

Variables	Probit Model		Logit Model	
	Coefficients (Standard Errors)	Marginal Effects (Standard Errors)	Coefficients (Standard Errors)	Marginal Effects (Standard Errors)
<i>category</i>	-0.1044 (0.0812)	-0.0416 (0.0324)	-0.1653 (0.1314)	-0.0413 (0.0328)
<i>platform</i>	0.0418 (0.0832)	0.0167 (0.0332)	0.0667 (0.1345)	0.0167 (0.0336)
<i>type</i>	-0.3921 *** (0.0870)	-0.1550 *** (0.0339)	-0.6305 *** (0.1405)	-0.1559 *** (0.0340)
<i>ads</i>	-0.0960 (0.1119)	-0.0382 (0.0445)	-0.1508 (0.1814)	-0.0376 (0.0451)
<i>iap</i>	0.5754 *** (0.1011)	0.2242 *** (0.0374)	0.9291 *** (0.1653)	0.2253 *** (0.0375)
<i>remuneration</i>	1.3280 ** (0.5259)	0.4176 *** (0.0928)	2.3011** (1.0490)	0.4199 *** (0.0928)
<i>constant</i>	0.0574 (0.08511)		0.0909 (0.1612)	
Log likelihood	-734.83821		-734.88165	
LR Chi ² (6)	83.61 ***		83.52 ***	

Note: N = 1121; ** Significant with p-value <0.05; *** Significant with p-value <0.01

Some of the variables that explained the disclosure of a privacy policy have a similar effect on the decision to explicitly inform about the use of personal data for micro-segmentation. To be paid decreases the probability of informing about the use of personal data for micro-segmentation by 15.50 percentage points (the effect was - 15.26 percentage points on the probability of *privacy* = 1). This result corroborates that if an app is paid for download the users will be less informed about the use of personal data, despite the disclosure or not of the privacy policy.

For apps with in-app purchases, the probability of an app to disclose the privacy policy is 13.06 percentage points higher and the probability of an app to inform about the use of personal data for micro-segmentation is 22.42 percentage points higher. Regression analysis shows that users of apps with in-app purchases are better informed about how the app uses their personal data, either because of higher probability of availability of privacy policy, and because privacy policies are more accurate and informative about the use of personal data for micro-segmentation. It seems that app developers which include in-app purchases are keener to adequately inform users. However, they do not have the same behavior concerning advertising. The existence of ads is not significant to explain the probability of explicitly informing users about the use of personal data for micro-segmentation. We may argue that, in the presence of ads, users expect that data is collected and used (Tang et al., 2022), and may adequate their choices and use of the app. Nonetheless, that does not substitute full disclosure for a well-informed decision.

Being in the “Medical Care/Medicine” category decreases the probability of having privacy policy available by 7.4 percentage points. However, the variable *category* is not significant to explain the probability of informing users about the use of personal data for micro-segmentation. Combining the availability of privacy policies and the accuracy of those policies, we conclude that there is no significant difference between how users are informed about the use of personal data for micro-segmentation.

Finally, remuneration of app users has a positive impact of 41.76 percentage points on the probability of informing about the use of personal data for micro-segmentation. The variable *remuneration* has no statistically significant impact on the disclosure of the privacy policy, but privacy policies are more accurate for the few apps that remunerate users, causing that positive impact on the variable *inform*. Therefore, apps that remunerate users disclose more information about the business model and what the roles of app owners and users are. Acknowledging that personal data is used and actively informing the benefits/remuneration that this may bring

to users can be a viable business strategy, based on the idea of the 'privacy calculus' (users are willing to share data in exchange for a gain). The benefit does not have to be exclusively monetary. Another type of benefits can be valued: the possibility of accessing social comparison mechanisms (comparing your personal data with the average of the group) can be an important factor for choosing a health app (Joeckel et al., 2021); or the possibility of participating in the creation or development of the app itself as it happens in digital games (El Afi and Ouiddad, 2021).

5. Conclusions and Policy Implications

There are many studies that describe the behavior of apps on privacy issues and use of personal data, however most of them lack to explain that behavior. Our work contributes to the comprehension of why some health apps do not have a privacy policy available and/or do not fully disclose on the use of personal data. We focused on business factors to explain the lack of privacy policies or accurate information in a sector where personal data is so sensitive.

We found that the pricing strategy and the presence of in-app-purchases are important to explain both the disclosure of a privacy policy and the information about the use of personal data for micro-segmentation. However, we did not find a significant effect on the presence of ads. Apps that remunerate users are more probable to explicitly inform users on the use of personal data for micro-segmentation purposes.

Our work tries to link privacy policies and their 'quality/accuracy' with the 'monetization of privacy capital'. However, precisely because many developers do not disclose detailed and reliable privacy policies, it is difficult to study this new monetization mechanism and its real weight and importance in many business models. However, evidence is enough to alert entrepreneurs that they should not ignore personal data as a strategic business variable.

Acknowledgements

This work was supported by national funds through FCT - Fundação para a Ciência e Tecnologia, I.P. under the project UNIAG UID/04752/2025 (DOI 10.54499/UID/04752/2025).

Ethics Declaration

There was no need for ethical clearance for the research referred to in this paper.

AI Declaration

AI tools were not used in the creation of this paper.

References

- Alamri, H., Maple, C., Mohamad, S., and Epiphaniou, G. (2022) "Do the Right Thing: A Privacy Policy Adherence Analysis of Over Two Million Apps in Apple iOS App Store", *Sensors*, v. 2222, pp. 8964. <https://doi.org/10.3390/s22228964>.
- Alfawzan, N., Christen, M., Spitale, G., and Biller-Andorno, N. (2022) "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis", *JMIR MHealth and UHealth*, v. 105, e33735. <https://doi.org/10.2196/33735>.
- Aydin, G., and Silahtaroglu, G. (2021) "Insights into Mobile Health Application Market Via a Content Analysis of Marketplace Data with Machine Learning", *PLOS ONE*, vol. 16, n.1, pp. 1–22. <https://doi.org/10.1371/journal.pone.0244302>
- Cameron, A. C., and Trivedi, P. K. (2008) *Microeconometrics Using Stata*, Stata Press.
- Cecere, G., Lefrere, V., & Le Guel, F. (2022) "Third parties in the app market and economics of privacy". *Economics Bulletin*, vol. 42, no. 2, pp. 1040-1049. <https://hal.science/hal-03948401>
- El Afi, F., and Ouiddad, S. (2021) "Consumer engagement in value co-creation within virtual video game communities", *Management & Marketing. Challenges for the Knowledge Society*, vol. 164, pp. 370-386. <https://doi.org/10.2478/mmcks-2021-0022>
- Fan, M., Yu, L., Chen, S., Zhou, H., Luo, X., Li, S., Liu, Y., Liu, J., and Liu, T. (2020) "An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps", In 2020 IEEE 31st international symposium on software reliability engineering ISSRE, pp. 253–264. <https://doi.org/10.1145/3626962>
- Gujarati, D. N., and Porter, D. C. (2011). *Econometria Básica*, The McGraw-Hill Companies.
- Han, C., Reyes, I., Elazari Bar On, A., Reardon, J., Feal, A., Egelman, S., and Vallina-Rodriguez, N. (2019) "Do you get what you pay for? comparing the privacy behaviors of free vs. paid apps", In *Workshop on Technology and Consumer*

- Protection ConPro 2019*, in conjunction with the 39th IEEE Symposium on Security and Privacy, San Francisco, CA, USA <http://hdl.handle.net/20.500.12761/691>.
- Iwaya, L. H., Babar, M. A., Rashid, A., and Wijayarathna, C. (2023) "On the privacy of mental health apps: An empirical investigation and its implications for app development", *Empirical Software Engineering*, v. 28, n.1, p.2. <https://doi.org/10.1007/s10664-022-10236-0>
- Joeckel, S., Henke, J., and Dogruel, L. (2021) "Trading Data for Health: How Social Comparison Orientation and Privacy Attitudes Impact on mHealth App Use", *European Journal of Health Communication*, vol. 23, pp. 62-84. <https://doi.org/10.47368/ejhc.2021.304>.
- Kollnig, K. (2021) "Tracking in apps' privacy policies". arXiv preprint arXiv:2111.07860. <https://doi.org/10.48550/arXiv.2111.07860>
- Laperdrix, P., Mehanna, N., Durey, A., and Rudametkin, W. (2022) "The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem", In *Proceedings of the ACM Web Conference 2022*, pp.3440-3449. <https://doi.org/10.1145/3485447.3512279>
- Lupiáñez-Villanueva, F., Folkvord, F., and Abeele, M. vanden. (2020) "Influence of the Business Revenue, Recommendation, and Provider Models on Mobile Health App Adoption: Three-Country Experimental Vignette Study", *JMIR MHealth and UHealth*, vol. 8, n. 6, e17272. [doi:10.2196/17272](https://doi.org/10.2196/17272)
- O'Loughlin, K., Neary, M., Adkins, E.C., and Schueller, S.M. (2019) "Reviewing the Data Security and Privacy Policies of Mobile Apps for Depression", *Internet Interventions*, vol. 15, pp. 110–115. <https://doi.org/10.1016/j.invent.2018.12.001>
- Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., and Patsakis, C. (2018) "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice", *IEEE Access*, vol. 6, pp.9390–9403. <https://doi.org/10.1109/ACCESS.2018.2799522>
- Polykalas, S.E., and Prezerakos, G.N. (2019) "When the mobile app is free, the product is your personal data. Digital Policy", *Regulation and Governance*, vol. 212, pp. 89-101. <https://doi.org/10.1108/DPRG-11-2018-0068>
- Story, P., Zimmeck, S., and Sadeh, N. (2018) "Which Apps have Privacy Policies? An Analysis of Over One Million Google Play Store Apps", In: Medina, M., A. Mittrakas, K. Rannenber, E. Schweighofer, & N. Tsuroulas, *Privacy Technologies and Policy*. APF 2018. Lecture Notes in Computer Science 11079. Springer, Cham. https://doi.org/10.1007/978-3-030-02547-2_1
- Sunyaev, A., Dehling, T., Taylor, P.L., and Mandl, K.D. (2015) "Availability and quality of mobile health app privacy policies", *Journal of the American Medical Informatics Association*, vol. 22e1, e28-e33. <https://doi.org/10.1136/amiainl-2013-002605>
- Tang, J., Shoemaker, H., Teffera, L., Birrell, E., and Lerner, A. (2022) "Buying Privacy: User Perceptions of Privacy Threats from Mobile Apps", *arXiv preprint arXiv:2211.07235*. <https://doi.org/10.48550/arXiv.2211.07235>
- Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., and Yuan, Q. (2021) "Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue", *Telematics and Informatics*, vol. 61, p. 101601. <https://doi.org/10.1016/j.tele.2021.101601>
- Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russel, N.C., and Sadeh, N. (2019) "Maps: Scaling privacy compliance analysis to a million apps", In *Proceedings on Privacy Enhancing Technologies*, vol. 66. https://ir.lawnet.fordham.edu/faculty_scholarship/1040