ENGENHARIAS, TECNOLOGIA, GESTÃO E TURISMO
ENGINEERING, TECHNOLOGY, MANAGEMENT AND TOURISM
INGENIERÍA, TECNOLOGÍA, ADMINISTRACIÓN Y TURISMO

millenium

Millenium, 2(Edição Especial Nº23)

DIVULGAÇÃO DE POLÍTICAS DE PRIVACIDADE E INFORMAÇÃO SOBRE O USO DE DADOS PESSOAIS, EM APLICAÇÕES DE SAÚDE

DISCLOSURE OF PRIVACY POLICIES AND INFORMATION ON THE USE OF PERSONAL DATA, ON HEALTH APPS

DIVULGACIÓN DE POLÍTICAS DE PRIVACIDAD E INFORMACIÓN SOBRE EL USO DE DATOS PERSONALES, EN APLICACIONES SANITARIAS

Cláudia Cardoso[1] https://orcid.org/0000-0003-2828-1652
Cândida Machado[1] https://orcid.org/0000-0002-4496-8879
Natália Lemos[1] https://orcid.org/0000-0003-2382-0645

[1] Instituto Politécnico do Cávado e do Ave, Barcelos, Portugal

Cláudia Cardoso - ccardoso@ipca.pt | Cândida Machado - cmachado@ipca.pt | Natália Lemos - nslemos@ipca.pt

Corresponding Author:
Cláudia Cardoso
Campus do IPCA
4750-810 – Barcelos - Portugal
ccardoso@ipca.pt

RECEIVED: 28th May, 2024
REVIEWED: 31st March, 2026
ACCEPTED: 17th April, 2026
PUBLISHED: 05th June, 2026

DOI: https://doi.org/10.29352/mill0223e.36159

RESUMO

Introdução: Evidência dos serviços online mostra que a proteção da privacidade ainda é um problema, e muitos desenvolvedores de aplicações falham na divulgação de uma política de privacidade ou na sua precisão.
Objetivo: Explicar como a disponibilidade da política de privacidade de uma aplicação de saúde e como a decisão de uma aplicação de informar explicitamente os utilizadores sobre o uso de dados pessoais para micro-segmentação se relacionam com diversas fontes de receita, tratando essas variáveis como variáveis estratégicas do negócio.
Métodos: Foi realizado um estudo transversal das aplicações de saúde disponíveis em Portugal. Usamos modelos de regressão *logit* e *probit* para estabelecer relações de causa-efeito entre variáveis.
Resultados: Constatamos que, se uma aplicação de saúde for descarregada gratuitamente ou incluir compras na aplicação, é mais provável que tenha uma política de privacidade e que os utilizadores sejam explicitamente informados sobre o uso de dados pessoais. No entanto, a inclusão de anúncios na aplicação não é relevante para explicar ambas as variáveis dependentes.
Conclusão: A divulgação de políticas de privacidade e o uso de dados pessoais não podem ser desconectados do modelo de negócios da aplicação.

Palavras-chave: política de privacidade, micro-segmentação, dados pessoais, aplicações de saúde, modelos de monetização

ABSTRACT

Introduction: Evidence from online services shows that privacy protection is still an issue, and many app developers fail in the disclosure of a privacy policy or in its accuracy.
Objective: 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 relate to 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-and-effect relations between variables.
Results: We found that 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 that users are explicitly informed about the use of personal data. However, the inclusion of ads within the app is not relevant to explain both dependent variables.
Conclusion: 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

RESUMEN

Introducción: La evidencia de los servicios en línea muestra que la protección de la privacidad sigue siendo un problema, y muchos desarrolladores de aplicaciones no revelan una política de privacidad o esto no es exacto.
Objetivo: Explicar cómo la disponibilidad de la política de privacidad de una aplicación de salud y cómo la decisión de una aplicación de informar explícitamente a los usuarios sobre el uso de datos personales para la microsegmentación se relacionan con diversas fuentes de ingresos, tratando estas variables como variables estratégicas de negocio.
Métodos: Se realizó un estudio transversal de las aplicaciones sanitarias disponibles en Portugal. Se utilizaron modelos de regresión logit y probit para establecer relaciones causa-efecto entre variables.
Resultados: Hemos descubierto que si una aplicación de salud se descarga de forma gratuita o incluye compras dentro de la aplicación, es más probable que tenga una política de privacidad y que los usuarios estén informados explícitamente sobre el uso de los datos personales. Sin embargo, la inclusión de anuncios in-app no es relevante para explicar ambas variables dependientes
Conclusión: La divulgación de las políticas de privacidad y el uso de datos personales no se pueden desvincular del modelo de negocio de la aplicación.

Palabras clave: política de privacidad, microsegmentación, datos personales, aplicaciones de salud, modelos de monetización

DOI: https://doi.org/10.29352/mill0223e.36159

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. Governments and 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.

Despite the evidence that many health app developers do not present a full-disclosure privacy policy, there is some evidence that transparency could be an important business strategy. In this paper, we intend to explain how the availability of the privacy policy of an app relates to 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 behaviour 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.

1. 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 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 (Spain, Germany, and the Netherlands), data protection increased the likelihood of downloading the app (Folkvord et al., 2023). Although Fan et al. (2024) found that the concern with privacy has a low impact on the willingness to use a mHealth app.

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, shows that privacy protection is still an issue, and many app developers fail to disclose a privacy policy. Moreover, even when the privacy policy is disclosed, many times it does not comply with what a privacy policy document should be, 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. 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. Alfawzan et al. (2022) showed that, of the 23 most popular women’s mHealth apps, 16 (70%) have a privacy policy. The study of Iwaya et al. (2023) revealed significant privacy and security issues regarding personal data for mental health apps, aggravated by the sharing of data with third parties, such as advertisers. The study of Magoulas and Polykalas (2023) reveals progress has been made towards achieving General Data Protection Regulation (GDPR) compliance, analysing before and after GDPR implementation in Europe, but full compliance was still far away. Cory et al. (2024), analysing 152 Android mHealth apps, reveal extensive issues, such as health data leakage to third-party trackers and a common disregard for privacy-by-design and transparency.

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 with the availability of privacy policies in health apps. The next step is to understand how app developers make the decision to disclose or not disclose 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 does not have 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 advertisements 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). 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.

DOI: https://doi.org/10.29352/mill0223e.36159

2. METHODS

2.1 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 (beginning of the research project that underpinned this article). 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	
privacy	Dummy variable that specifies if the privacy policy is available (if not = 0; if so = 1)
inform	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	
type	Dummy variable that identifies the typology of the app (Free = 0; Paid = 1)
iap	Dummy variable that specifies whether the app has in-app purchase options (if not = 0; if so =1)
ads	Dummy variable that specifies whether the app has ads (if not = 0; if so =1)
remuneration	Dummy variable that identifies if the app remunerates the users (if not = 0; if so = 1)
platform	Dummy variable that identifies the platform where the app is marketed (Google Play Store = 0; Apple App Store = 1)
category	Dummy variable that specifies the category in which the app is classified ("Health and Fitness" = 0; "Medical Care/Medicine" = 1)

2.2 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 a privacy policy available (*privacy*=0) and the sub-sample of apps with a 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. In the full sample, 71.63% of the health apps disclose their privacy policy. Additionally, the variable *inform* shows if the users are explicitly informed that their personal data is used for micro-segmentation of advertising (by the app developer or by third parties). If *inform* equals zero, it means that users are not informed, either because the privacy policy is not available or the use of personal data is not explicitly addressed in the privacy policy. If *inform* equals one, it means that users are explicitly informed whether their personal data is used or not for micro-segmentation. Concerning this, 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).

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)
privacy =1	71.63%	------	-----	44.70%	100.00%
inform = 1	48.71%	0.00%	68.00%	------	-----
type = 1	38.54%	52.20%	33.13%	47.30%	29.30%
iap = 1	20.79%	11.64%	24.41%	12.70%	29.30%
ads =1	18.29%	15.41%	19.43%	15.48%	21.25%
remuneration =1	1.16%	0.31%	1.49%	0.17%	2.20%
platform =1	40.95%	41.19%	40.85%	41.73%	40.11%
category =1	64.94%	72.33%	62.02%	68.17%	61.54%

The variable *inform* is zero for all the apps without a 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 a privacy policy and the sub-sample of apps that "do not inform" have higher percentages of "Medical Care/Medicine" apps.

DOI: https://doi.org/10.29352/mill0223e.36159

The health apps on the sample are available on the two major platforms operating in Portugal: Apple App Store (with 40.95% of the observations) and Google Play Store (with 59.05% of the observations). The distribution is similar in 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 a privacy policy, there is a higher percentage of paid apps than in the full sample. For apps with a 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 in the group of apps without a 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 includes 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 significant number of users and/or their engagement (which may guarantee advertising revenues) or to pay for personal data.

We do not have data for a possible fourth source of revenue: selling personal data to third parties (and/or using their personal data for targeting advertising and in-app purchases more efficiently). Yet, we know if the users are explicitly informed of the use of personal data for micro-segmentation (*inform*). We cross that information with our data on revenue sources in Table 3.

Table 3 - Sources of revenue and the use of data for micro-segmentation

Sources of revenue	N	Remunerate users	Using personal data for micro segmentation		
			Inform		Do not inform
			Use	Do not use	
Ads	113	1	0	58	55 (22 with PP)
Ads + IAPs	91	2	0	57	34 (18 with PP)
Ads + IAPs + Paid	0	0	0	0	0
IAPs	103	0	1	75	27 (14 with PP)
IAPs + Paid	39	0	0	27	12 (4 with PP)
Paid	392	0	30	102	260 (102 with PP)
Ads + Paid	1	0	0	1	0
None	382	10	6	189	187 (97 with PP)
	1121	**13**	**37**	**509**	**575**

Note: with PP – with privacy policy available

Only 37 health apps inform that they use the personal data for micro-segmentation (3.3% of total). The most surprising is that, from those 37 apps, 30 apps are paid. Paying for the app does not guarantee that personal data will not be collected and used for commercial purposes.

There are 509 apps (45.41% of the total) that explicitly state that they do not use personal data for micro-segmentation. Since the use of personal data for micro-segmentation can potentiate the revenues of ads and in-app purchases, it was expected that apps that solely rely on those sources of revenue (Ads, Ads+IAPs, IAPs) would have higher use of personal data. However, 61.88% of those apps explicitly inform that they "do not use". From the apps that include payment for download (Ads+IAPs+Paid, IAPs+Paid, Paid, Ads+Paid), 30.1% explicitly inform that they "do not use". There are 189 health apps (from a total of 382) that inform that they do not use personal data for micro-segmentation, and they do not have any of the three sources of revenue mentioned. We can only speculate on the business model of those apps: they may be at an early stage, and they want to get as many users as possible and then introduce ads or in-app purchases; they may be a tool to achieve other business goals within a firm with several activities interconnected; or they may be collecting and using personal data for other purposes than micro-segmentation.

Finally, we have 575 health apps (51.29% of the total) that do not inform about the use of personal data for micro-segmentation. Within this group, we have 318 apps (28.37% of total apps) that do not inform because they do not have a privacy policy available, and 257 apps (22.93% of total apps) that do not inform despite having a privacy policy available. Paid apps without ads or in-app purchases are the group of apps where the lack of information is higher, followed by the group of apps with none of the three sources of revenue.

2.3 Regression analysis

We analyse the factors that influence the likelihood of disclosure of the 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

DOI: https://doi.org/10.29352/mill0223e.36159

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 & 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 & Trivedi, 2008).

3. RESULTS AND DISCUSSION

As mentioned above, we use logit and probit regression models to establish how the independent variables explain the behaviour of our dependent variables: *privacy* and *inform*. Regression techniques enable us to understand the cause-and-effect relations, controlling for the other variables to be constant.

3.1 Dependent variable *privacy*

Results for the dependent variable *privacy* are presented in Table 4. Results are similar for both regression models. However, considering the log likelihood value of the logit and probit models, Table 4 shows that the most appropriate probability model is the probit, whose log likelihood is -638.2008, that is, the highest value.

Table 4 - 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)
category	-0.2276 **	-0.0740 ***	-0.3784 **	-0.0726 ***
	(0.0880)	(0.0279)	(0.1492)	(0.0277)
platform	0.0967	0.0320	0.1547	0.0303
	(0.0881)	(0.0290)	(0.1473)	(0.0287)
type	-0.4480 ***	-0.1526 ***	-0.7431 ***	-0.1514 ***
	(0.0915)	(0.0316)	(0.1535)	(0.0318)
ads	-0.1605	-0.0549	-0.2685	-0.0550
	(0.1225)	(0.043)	(0.2086)	(0.0442)
iap	0.4284 ***	0.1306 ***	0.7456 ***	0.1317 ***
	(0.1146)	(0.0314)	(0.2029)	(0.0312)
remuneration	0.5895	0.1576	1.0697	0.1588
	(0.5291)	(0.1051)	(1.0509)	(0.1070)
constant	0.8179 ***		1.3428 ***	
	(0.0942)		(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

First, the *category* is a statistically significant variable. Being in the "Medical Care/Medicine" category decreases the probability of having a privacy policy available by 7.4 percentage points. This result is in line with Alamri et al. (2022). Although previous studies were not able to prove the effect of those categories on the disclosure of privacy policies (Story et al., 2018). 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. In 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 the 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 a privacy policy.

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 the 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 sharing 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 (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,

DOI: https://doi.org/10.29352/mill0223e.36159

the variables *ads* and *iap* have different impacts 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 a privacy policy available by 13.06 percentage points. This result is in accordance with Kollnig (2021), who showed that apps, relying on in-app purchases as a revenue source, harvest personal data and, therefore, may be more aware of the need for a privacy policy to maintain users' confidence. Story et al. (2018) showed that more than 65% of apps with in-app purchases have a link to their privacy policy, and that was the interactive element that contributed more to having a privacy policy available.
Finally, to remunerate users has a positive but not statistically significant effect on the availability of the 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 in 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.

3.2 Dependent variable *inform*

As for the dependent variable *inform*, estimation results are exhibited in Table 5. Results are similar for both regression models, but we will analyse the results of the probit model, whose log likelihood is -734.83821, which is the highest value.

Table 5 - 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)
category	-0.1044	-0.0416	-0.1653	-0.0413
	(0.0812)	(0.0324)	(0.1314)	(0.0328)
platform	0.0418	0.0167	0.0667	0.0167
	(0.0832)	(0.0332)	(0.1345)	(0.0336)
type	-0.3921 ***	-0.1550 ***	-0.6305 ***	-0.1559 ***
	(0.0870)	(0.0339)	(0.1405)	(0.0340)
ads	-0.0960	-0.0382	-0.1508	-0.0376
	(0.1119)	(0.0445)	(0.1814)	(0.0451)
iap	0.5754 ***	0.2242 ***	0.9291 ***	0.2253 ***
	(0.1011)	(0.0374)	(0.1653)	(0.0375)
remuneration	1.3280 **	0.4176 ***	2.3011**	0.4199 ***
	(0.5259)	(0.0928)	(1.0490)	(0.0928)
constant	0.0574		0.0909	
	(0.08511)		(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 of -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 whether the privacy policy.
For apps with in-app purchases, the probability of an app disclosing the privacy policy is 13.06 percentage points higher, and the probability of an app informing 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 a higher probability of availability of privacy policy, or because privacy policies are more accurate and informative about the use of personal data for micro-segmentation. It seems that app developers who include in-app purchases are keener to adequately inform users. However, they do not have the same behaviour concerning advertising. The existence of ads is not significant in explaining 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), which may affect 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 a privacy policy available by 7.4 percentage points. However, the variable *category* is not significant in explaining the probability to inform users about the use of personal data for micro-segmentation. Combining the availability of the privacy policies and the accuracy of those policies, we conclude that there is no significant difference in how users are informed about the use of personal data for micro-segmentation.

DOI: https://doi.org/10.29352/mill0223e.36159

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 a positive impact on the variable *inform*. Therefore, apps that remunerate users disclose more information about the business model and what are the roles of app owners and users. 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 benefit 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 & Ouiddad, 2021).

CONCLUSION

There are many studies that describe the behaviour of apps on privacy issues and the use of personal data; however, most of them lack to explain that behaviour. Our work contributes to the comprehension of why some health apps do not have a privacy policy available and/or do not fully disclose 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 for the presence of ads. Apps that remunerate users are more likely to explicitly inform users of 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. Future research should focus more on how personal data is a strategic business variable and how health app business models affect the privacy and security of personal data.

ACKNOWLEDGEMENTS

We acknowledge the support of the Project “NORTE-01-0145-FEDER-000045”, supported by Northern Portugal Regional Operational Programme (Norte2020), under the Portugal 2020 Partnership Agreement, through the European Regional Development Fund (ERDF).

AUTHORS' CONTRIBUTION

Conceptualization, C.C. and C.M.; data curation, N.L.; formal analysis, C.C., C.M. and N.L.; funding acquisition, C.C., C.M. and N.L.; investigation, C.C., C.M. and N.L.; methodology, C.C., C.M. and N.L.; project administration, C.C. and C.M.; supervision, C.C. and C.M.; validation, C.C. and C.M.; writing – original draft, C.C. and C.M.; writing – review and editing, C.C., C.M. and N.L.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

REFERENCES

Alamri, H., Maple, C., Mohamad, S., & Epiphaniou, G. (2022). Do the right thing: A privacy policy adherence analysis of over two million apps in Apple iOS app store. *Sensors*, *2222*, 8964. https://doi.org/10.3390/s22228964.

Alfawzan, N., Christen, M., Spitale, G., & 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*, *105*, e33735. https://doi.org/10.2196/33735.

Aydin, G., & Silahtaroglu, G. (2021). Insights into Mobile Health Application Market Via a Content Analysis of Marketplace Data with Machine Learning. *PLOS ONE*, *16* (1), 1–22. https://doi.org/10.1371/journal.pone.0244302 .

Cameron, A. C., & Trivedi, P. K. (2008). *Microeconometrics using stata* (1st Ed.). Stata Press.

Cecere, G., Lefrere, V., & Le Guel, F. (2022). Third parties in the app market and economics of privacy. *Economics Bulletin*, *42*(2), 1040-1049. https://hal.science/hal-03948401

DOI: https://doi.org/10.29352/mill0223e.36159

Cory, T., Rieder, W., & Huynh, T. M. (2024). A qualitative analysis framework for mhealth privacy practices. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 24-31). IEEE. https://doi.org/10.1109/EuroSPW61312.2024.00010

El Afi, F., & Ouiddad, S. (2021). Consumer engagement in value co-creation within virtual video game communities. *Management & Marketing. Challenges for the Knowledge Society*, *164*, 370-386. https://doi.org/10.2478/mmcks-2021-0022

Fan, S., Jain, R. C., & Kankanhalli, M. S. (2024). A comprehensive picture of factors affecting user willingness to use mobile health applications. *ACM Transactions on Computing for Healthcare*, *5(*1), 1-31. https://doi.org/10.1145/3626962

Folkvord, F., Bol, N., Stazi, G., Peschke, L., & Lupiáñez-Villanueva, F. (2023). Preferences in the willingness to download an mHealth app: discrete choice experimental study in Spain, Germany, and the Netherlands. *JMIR Formative Research*, *7(*1), e48335. doi: 10.2196/48335

Gujarati, D. N., & Porter, D. C. (2011). *Econometria Básica* (5a Edição). The McGraw-Hill.

Iwaya, L. H., Babar, M. A., Rashid, A., & Wijayarathna, C. (2023). On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering*, *28*(1), 2. https://doi.org/10.1007/s10664-022-10236-0

Joeckel, S., Henke, J., & Dogruel, L. (2021). Trading data for health: How social comparison orientation and privacy attitudes impact on mHealth app use. *European Journal of Health Communication*, *23*, 62-84. https://doi.org/10.47368/ejhc.2021.304.

Kollnig, K. (2021). Tracking in apps' privacy policies. *arXiv preprint.* https://doi.org/10.48550/arXiv.2111.07860

Laperdrix, P., Mehanna, N., Durey, A., & 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

Magoulas, G. S., & Polykalas, S. E. (2023). Access to personal data is still tempting for mobile apps even after the GDPR implementation. In *2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference* (SEEDA-CECNSM) (pp. 1-6). IEEE. https://doi.org/10.1109/SEEDA-CECNSM61561.2023.10470645

O'Loughlin, K., Neary, M., Adkins, E.C., & Schueller, S.M. (2019). Reviewing the data security and privacy policies of mobile apps for depression. *Internet Interventions*, *15*, 110–115. https://doi.org/10.1016/j.invent.2018.12.001

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, *6*, 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

Story, P., Zimmeck, S., & Sadeh, N. (2018). Which apps have privacy policies? An analysis of over one million Google Play Store apps. In M. Medina., A. Mitrakas, K. Rannenberg, E. Schweighofer, & N. Tsouroulaseds. (Eds.), *Privacy Technologies and Policy (APF 2018)* (Lecture Notes in Computer Science, Vol. 11079). Springer. https://doi.org/10.1007/978-3-030-02547-2_1

Tang, J., Shoemaker, H., Teffera, L., Birrell, E., & Lerner, A. (2022). Buying privacy: User perceptions of privacy threats from mobile apps. *arXiv preprint.* https://doi.org/10.48550/arXiv.2211.07235

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, *61*, 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., & Sadeh, N. (2019). Maps: Scaling privacy compliance analysis to a million apps. In *Proceedings on Privacy Enhancing Technologies*, *66.* https://ir.lawnet.fordham.edu/faculty_scholarship/1040