FACULTY OF
MANAGEMENT & FINANCE
UNIVERSITY OF COLOMBO

Colombo
Business
Journal

INTERNATIONAL JOURNAL OF
THEORY & PRACTICE
Vol. 14, No. 02, December, 2023

Impact of Users' Comprehension of the Privacy Policy of FemTech Apps on their Information Disclosure Intentions: The Mediating Effects of Privacy Fatigue and Privacy Data Control

Neethu Mohan[a]✉, K. A. Zakkariya[b]

[ab]School of Management Studies, Cochin University of Science and Technology, India

Abstract

FemTech stands for female technology, which encompasses a wide range of software, products, and services designed to improve women's health through technology. Personal data used in this type of app are intimate, which highlights the importance of privacy, and therefore, comprehensibility of the privacy policies of such apps. This study explores the effect of user comprehension of privacy policies on their information disclosure intention through mediators such as privacy fatigue and privacy data control, which have rarely been studied. A scenario-based questionnaire was used to collect data from 236 females and SMART PLS 4.0 was used to conduct the analysis. Findings indicate that both mediators have an indirect-only mediation effect; however, the direction of the impact of privacy fatigue on disclosure intention was opposite to what was hypothesised. Privacy data control was found to be the stronger mediator. This study entails implications for privacy policymakers and mobile health application providers.

***Keywords*:** Privacy Policy Comprehension, Privacy Fatigue, Privacy Data Control, FemTech, Disclosure Intention

Received:	Accepted revised version:	Published:
26 December 2022	11 October 2023	31 December 2023

Suggested citation: Neethu M. & Zakkariya, K.A. (2023). Impact of users' comprehension of the privacy policy of FemTech apps on their information disclosure intentions: The mediating effects of privacy fatigue and privacy data control. *Colombo Business Journal, 14*(2), 132-156.

DOI: https://doi.org/10.4038/cbj.v14i2.160

✉ nmohan2906@gmail.com https://orcid.org/0000-0002-0541-3475

Introduction

Mobile phones are powerful multifunctional devices that are capable of doing more than just communicating. Much attention is being drawn to mobile technology, especially smartphones, and many new applications are developed and launched daily that address unique needs in new areas (Zolkepli et al., 2021). In the healthcare industry, mobile technology is gaining attention, which is generally referred to as mobile health (or mHealth), which refers to providing health services through mobile devices (Zhu et al., 2021). Even several years back, there were estimated to be over 165,000 mHealth apps (Mishra, 2015).

In this study, the subject of interest was menstrual tracking apps, under the category of mHealth apps. Apps for tracking periods fall under the category of FemTech, a growing market that focuses on the needs of women and their overall well-being through technological solutions and ancillary services (Bansal, 2021). To provide the promised service, menstrual tracking apps require private information (Fowler et al., 2020). Although these applications provide several advantages to women and allow them to prepare for their period in advance, some questions remain about the accuracy, privacy claims, and in some cases, accessibility of these applications (Narayan, 2022).

A privacy policy is the only means through which app makers communicate to their users the data that they collect, and the use made of that data (Ermakova et al., 2015; Fowler et al., 2020). Even though many users are concerned with the privacy of their personal information, they rarely read privacy policies before using a service or making a purchase (Aïmeur et al., 2016; Gerlach et al., 2015). Privacy policies are often difficult to read and understand largely due to their length and complexity (Zhu et al., 2021). It is critical to present privacy policies in a friendly format because they are the primary source of information and the place where users consent to the practices about their privacy (Aïmeur et al., 2016; Aïmeur & Lafond, 2013). It is important to emphasise here that users are practically forced to accept the terms of the policy in order to utilise the service (Furnell & Phippen, 2012). In this situation, users are often faced with a dilemma where they have to choose between two unappealing alternatives (Aïmeur et al., 2016). Either the user accepts the terms of the policy at the risk of losing their privacy or the user refuses to comply with the policy in which case they are unable to use the service (Aïmeur et al., 2016; Capistrano & Chen, 2015). Even though privacy policies play a vital role in individuals' decision-making with respect to the intention to disclose information while using any mobile applications, it is observed that the required attention is not

given by people towards privacy policies, a key reason for which is the difficulty to comprehend privacy policies (Fowler et al., 2020; Tesfay et al., 2018). FemTech apps are a type of app that requires intimate information (Siapka & Biasin, 2021; Fowler et. Al, 2020). Therefore, the need for the prospective app user to understand what information is required and how the information will be used is high, and this information can only be found in the privacy policies (Fowler et.al, 2020). This highlights the pivotal role of privacy policies in the FemTech applications. If there is an easily comprehensible privacy policy in a FemTech app, it could produce a fruitful outcome for the app providers. The literature with respect to data practices in the FemTech category apps is at its infancy stage and is slowly growing (Bansal, 2021; Fowler et. al, 2020; Siapka & Biasin, 2021). The present study focuses on how the user comprehension of the privacy policies but also how privacy fatigue and privacy data control have an impact on the user's disclosure intention while using any menstrual tracking app, which has rarely been studied with respect to FemTech category apps.

Past literature indicates that there exists an interesting relationship between personalisation and privacy which is mainly a trade-off (Awad & Krishnan, 2006; Zhu et al., 2021), where the users are torn between the benefits that they receive when they avail of any service at the stake of their disclosure of personal information. The personalisation-privacy paradox tends to create a difference between the intended and the actual behaviour, that is, the prospective users are at conflict in their minds while disclosing personal information because they are taking a risk of disclosing their personal information with an expectation to receive the desired benefit from using the app (Awad & Krishnan, 2006; Zeng et al., 2021). These privacy concerns in the minds of the users could be reduced when presented with a user-friendly, easily comprehensible privacy policy. Thus, this paper attempts to address the issue empirically, by finding answers to the research question 'Does perceived comprehension of privacy policies influence users' intention to disclose information on menstrual tracking apps? and the paper also addresses the questions, 'Do privacy fatigue and privacy data control parallelly mediate the relationship between perceived comprehension of privacy policies and user's intention to disclose information, and, 'If parallel mediation exists, which of the mediation paths is stronger?'

Privacy data control could be a critical point when it comes to information disclosure on apps like menstrual tracking apps. Users can manage the data that they wish to exchange with the application using a privacy policy that is presented in a user-friendly manner (Capistrano & Chen, 2015; Guo et al., 2022). Therefore, this

paper hypothesises that users' perceived control over their data can be facilitated by an easily comprehensible privacy policy, which can then encourage them to disclose information. In a contrasting manner, past literature also suggests that the language and terms used in the privacy policies in general, be it the website privacy policies or the app privacy permissions, are difficult for the users to comprehend, that is, it creates privacy fatigue, and it is more convenient for them just to click accept and proceed (Ermakova et al., 2015; Obar & Oeldorf-Hirsch, 2018). In other words, privacy fatigue would increase users' intention to share information (Tang et al., 2020; Zhu et al., 2021). Thus, this paper hypothesises that privacy fatigue will negatively mediate the impact of perceived comprehension of a privacy policy on disclosure intention.

The paper is organised as follows: first the literature review consisting of disclosure intention and the underlying mechanisms of privacy policies. Second, the research hypotheses and the proposed conceptual model. Third, the research methodology and the analyses results and at last, the key findings, implications and the future scope for research.

Literature Review

Information Disclosure Intention in FemTech Apps

The FemTech movement has come a long way over the years to ensure women are at the centre of the design and development of such systems. This is due to a lack of data about women in general and bias and discrimination in health studies, data sets, and algorithms (Mehrnezhad et. al. 2022). Despite this, security, privacy, and safety remain major concerns in the FemTech industry (Mehrnezhad et. al. 2022). Since data used in FemTech technology is highly sensitive, issues related to safety and privacy might lead to catastrophic consequences.

As discussed earlier, FemTech apps require users' intimate information to provide them with the benefits of the app (Fowler et al., 2020; Siapka & Biasin, 2021). Based on the information, these apps could provide personalised service to their users. It is important to remember that in requesting information from users, an impasse arises between the personalisation and privacy of the user because to increase the quality of personalised services, it is necessary to provide personal information (Lee & Rha, 2016). Personalisation in healthcare settings involves the acquisition and re-use of user information (Lee & Rha, 2016). As such, the ability to personalise a service is subject to a trade-off with the ability to preserve privacy. If individuals are asked to provide personal information, they may anticipate that their privacy may be

compromised eventually leading to concerns with respect to their privacy (Lee & Rha, 2016). An individual may prefer to have control over how their personal information is disclosed to others, as well as how that information is used by others (Lee & Rha, 2016).

The literature on the online disclosure of information is generally fragmented and lacks conclusive evidence. Most of the literature pertaining to online information disclosure is in the e-commerce context (Awad & Krishnan, 2006; Dinev & Hart, 2006; Li et al., 2011; Zhu et al., 2017) and there are few studies in the context of health care apps in general (Ermakova et al., 2015; Zhu et al., 2021). Studies have also been conducted on the effects of privacy policies and assurances, web seals of approval, and other privacy initiatives on consumer information disclosure (Angulo et al., 2012; Earp et al., 2005; Miyazaki & Krishnamurthy, 2002; Xie et al., 2006). However, so far, there is little empirical evidence on the effect of privacy policy comprehension on information disclosure in the context of FemTech apps, taking into consideration 'Privacy Fatigue' and 'Privacy Data Control'.

Privacy Policies

A privacy policy explains how a website or mobile application collects and uses data about its users. Many studies show that users ignore these policies. According to a recent Deloitte survey of 2,000 consumers, 91% of consumers agree to legal terms and service conditions without reading them. The rate is significantly higher for younger individuals (18 to 34), with 97% of them consenting to terms before reading (Cakebread, 2017). Even if someone wanted to be assiduous, according to the study, it would require at least 76 workdays to read all the privacy policies they encounter (Medine & Murthy, 2019).

It is essential for users to understand how companies collect, use, and share their data. According to Aïmeur et al. (2016), their interpretation of the language of privacy policies differs significantly, primarily concerning data sharing. As a result, privacy policies can sometimes be unfair and lead to misinformed decisions. Furthermore, systems and applications integrated with social networks increase the lack of understanding of privacy policies (Aïmeur et al., 2016; Caramujo & Silva, 2015). Therefore, although a small number of people do examine privacy policies, they are often unable to assess adequately the consequences of collecting, using, or disclosing their personal information even if they take the time to do so (Aïmeur et al., 2016; Aïmeur & Lafond, 2013). Past evidence suggests that the main hurdle in understanding the privacy policy is the ability of the user to comprehend the privacy policy due to its complex language and content.

The information format of privacy policies refers to how information about the available alternatives and their characteristics are communicated and organised (Aïmeur et al., 2016; Cooper-Martin, 1993). When it comes to making a purchase, consumers assign importance to various attributes based on the way the product is presented, which in this case is the menstrual tracking app (Aïmeur & Lafond, 2013). When prospective users read the privacy policy, it influences their intention to disclose personal information in order to use the app. Therefore, changing user perception is key to enabling them to trust menstrual tracking apps with regard to their personal information. Furthermore, it will also affect their behaviour when, for instance, deciding what private data they are willing to share with menstrual tracking apps.

The present study tries to understand whether an easily comprehensible privacy policy could have a positive impact on the disclosure intention of the users through the mediating effects of 'Privacy Fatigue' and 'Privacy Data Control'.

Hypothesis Development and Conceptual Model

Comprehension and Disclosure Intention

Despite privacy policies being considered an important source of information for users, do people really understand privacy policies? Privacy policies can be unfair when they are not understood correctly and may lead people to make unfavourable privacy decisions (Aïmeur & Lafond, 2013; Wilson et al., 2016). Unfortunately, some privacy policies purposefully use confusing language and are written to prevent privacy lawsuits rather than addressing user privacy concerns (Aïmeur et al., 2016). Thus, the more comprehensible a privacy policy is, the more the user will be interested in reading it and intend to disclose information. Thus, we propose,

H_1: Comprehension has a positive impact on the disclosure intention

Comprehension, Privacy Fatigue and Disclosure Intention

In the context of online privacy, a growing number of privacy assurance protocols which are becoming increasingly complex, require users to spend more cognitive energy understanding those which tend to create fatigue in the mind of the users with respect to privacy, which is termed as 'Privacy Fatigue' (Keith et al., 2014). Privacy fatigue is based on the feature fatigue theory (Keith et. al., 2014). Although the feature fatigue theory is specifically applied to physical technology products, it has applications in the digital realm, such as mobile apps and websites. Each digital product has privacy controls that allow consumers to share their personal information.

The theory emphasises the notion that over time, there arises a trade-off between product capability and ease of use when the number of privacy features is increased due to the dynamic technological scenario (Keith et al., 2014). As the number of privacy controls increases, there is a tendency for users to get a feeling of fatigue towards the privacy control measures. Keith et al. (2014) have developed the term 'Privacy Fatigue' from the feature fatigue theory and tries to emphasise that, although the increase of privacy control features tends to increase the users' ability to control their privacy, it could also make them tired or fatigued. In this study, the feature fatigue theory is applied to the complexity of the policy with respect to the amount of information provided and the control measures provided to the users.

In a situation where the users are presented with an easily comprehensible privacy policy, it could have a negative impact on privacy fatigue (Zhu et al., 2021), since the mismatch between people's capabilities to understand the app mechanisms with respect to privacy has been suggested as a cause of fatigue in previous studies (Maslach, 2001; Zhu et al., 2021). This sense of fatigue could be reduced with an easy comprehensible privacy policy which will eventually enable the users to strengthen their beliefs in privacy rights. Thus, we propose,

H_2: There is a negative impact of comprehension on privacy fatigue

Interestingly, some literature on privacy fatigue suggests that fatigue could actually result in greater readiness to disclose information. This literature suggests that users may simply decide to disclose information as a negative coping mechanism for protecting themselves. The experience of privacy fatigue is often characterised by both emotional exhaustion as well as cynicism, which is often caused by an inability to achieve expectations in a timely manner (Choi et al., 2018). Cynicism toward online privacy is characterised by uncertainty, powerlessness, and distrust (Choi et al., 2018; Lutz et al., 2020). This problem is exacerbated when users lose confidence in the privacy of their data and feel dissatisfied with their online experience owing to privacy cynicism (Hoffmann et al., 2017; Zhu et al., 2021). When stressed or threatened, users act actively to reduce their stress by altering what they think about the problem (Strachan et al., 2009).

People who are fatigued tend to make fewer decisions. For example, privacy fatigue may inhibit them from making decisions regarding privacy (Lutz et al., 2020). According to Choi et al. (2018), people experiencing high levels of privacy fatigue do not take action to prevent misuse of their personal information. This could be because users may not be willing to invest considerable effort into managing their

personal information due to privacy fatigue (Choi et al., 2018). During the age of information, user information has become more readily accessible to others, and users are free to share their personal information for a wide range of services (Degryse & Bouckaert, 2006). As a result, protecting user privacy is difficult and complex privacy management processes are time-consuming and draining (Choi et al., 2018; Zhu et al., 2021). Users are wearied and powerless when it comes to privacy issues due to privacy fatigue (Hargittai & Marwick, 2016; Zhu et al., 2021). It is common for users who exhibit privacy cynicism to adopt the simplest method of handling the issue. For example, accepting default privacy settings is one way to do so (Schomakers et al., 2019). Furthermore, past literature found that privacy fatigue positively impacts privacy disclosure intentions (Choi et al., 2018; Zhu et al., 2021). Hence, users are more likely to disclose their personal information to the system when they are tired of privacy issues. Thus, we propose,

H_3: There is a positive impact of privacy fatigue on disclosure intention

The above two hypotheses with respect to privacy fatigue indicate a mediating effect between user comprehension of privacy policies and their disclosure intention, where greater comprehension of a privacy policy may actually reduce users' disclosure intention by reducing privacy fatigue.

The next section discusses a competing parallel mediation where greater comprehension of a privacy policy would increase disclosure intention through increasing privacy data control.

Comprehension, Privacy Data Control and Disclosure Intention

In 2018, the European Union implemented the General Data Protection Regulation (GDPR) which is considered to be the toughest privacy law on land (Wolford, 2018). The main pillars of GDPR are lawfulness, transparency and fairness. Privacy data control is also a major part of this law where the power is given to the users to control their data and also withdraw their data whenever they feel like it (Wolford, 2018). Users' permission must be explicitly requested, and all website settings must respect privacy (Aïmeur et al., 2016; Rotenberg & Jacobs, 2013). These types of laws are now being adopted by other regions of the world. For example, in India (a South Asian country), transparency (prior notice and privacy policy explaining how data is processed) is among the key tenets of the law in the latest draft of the Data Protection Bill of 2021 (Wadhwa & Bains, 2022). This makes it easier for individuals to remove, correct, and access their data (Wadhwa & Bains, 2022). In

other words, it would give them more control over their data (Aïmeur et al., 2016). For example, a privacy policy could provide an option of opt-out where the users have control over their data (Degryse & Bouckaert, 2006). An individual's right to control his or her information is related to understanding who uses it and why. It is crucial for the user to receive clear explanations before giving permission to be tracked (Aïmeur et al., 2016; Rotenberg & Jacobs, 2013). Thus, we propose,

H_4: There is a positive impact of comprehension on privacy data control

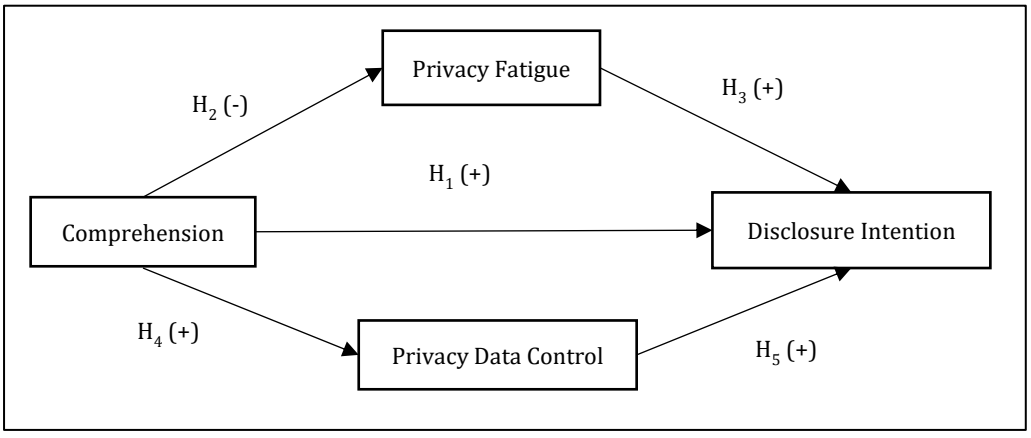
A company that provides better information about the usage and protection of their data will have a greater chance of winning the trust of users (Aïmeur et al., 2016). Users may be more likely to trust menstrual tracking mobile apps if they provide greater transparency regarding their private information and enable them to regain control of their information (Aïmeur et al., 2016; Degryse & Bouckaert, 2006). Providing greater control of data to the users will enable them to change their perspective towards the privacy management of these health-based apps (Aïmeur et al., 2016). Thus, we propose,

H_5: Privacy data control has a positive impact on disclosure intention

The above two hypotheses indicate the mediating effect of privacy data control between the users comprehension of privacy policies and their disclosure intention.

Figure 1 depicts the conceptual framework of this study based on the relationships hypothesised above.

Figure1: Conceptual Framework



Methodology

Data Collection

The inclusion criteria for the data collection considered are 1). Females who are in their menstrual phase and 2). Females, who under real circumstances, would be willing to install the menstrual tracking mobile application. A scenario-based questionnaire was used to collect the data. The scenario (see Appendix) included an excerpt of the privacy policy of a menstrual tracking app named 'FLO' and the image of the privacy portal of the same mobile app enlisting the basic guiding principles of the privacy policy for better understanding and comprehension. In the excerpt of the privacy policy, at the end, there was an opt-out option as well. At last, there was a question asked after reading the excerpt of the privacy policy and seeing the image of the privacy portal, "would you under real circumstances, install the above mentioned menstrual tracking mobile app?" The respondents were guided to fill out the questionnaire only if they answered 'yes'; otherwise, they were guided to exit the questionnaire.

As explained above the sample was selected based on the inclusion criteria set and was reached through online means, that is, an online questionnaire was sent to the females belonging to the menstrual age group and those who have shown interest in installing the menstrual tracking app were selected as the sample. Thus, the judgemental sampling method was used to reach the respondents.

Population and Sampling

The absence of a sampling frame necessitated a judgemental sampling approach The most widely used minimum sample size estimation method in PLS-SEM, in the field of Information Systems as well as other fields, is the "10-times rule" method (Hair et al., 2011; Peng & Lai, 2012). Among the variations of this method, the most commonly seen is based on the rule that the sample size should be greater than 10 times the maximum number of inner or outer model links pointing at any latent variable in the model (Goodhue et al., 2012). In our study, the maximum number of inner or outer model links pointing at a latent variable is 5 which means 10 times of 5 is 50, hence, the minimum sample size is 50. Although PLS is well known for its capability of handling small sample sizes, it does not mean that your goal should be to merely fulfil the minimum sample size requirement.

Therefore, approximately 321 females received the questionnaire and among them, 236 were willing to install the menstrual tracking mobile app. The age of the

respondents ranges from 15 to 40. Regarding educational qualifications, 61.3% of the participants were post-graduates and some college graduates (32.6%). Among the respondents, 40.3% stated that they have a prior experience with menstrual tracking app.

Measures

The measurement scales used for the constructs are presented in Table 1. All the constructs are reflective in nature. Seven-point Likert scales were used to measure the constructs. The three-item scale for user comprehension was adopted from Aïmeur et al. (2016). Privacy fatigue was measured using the scale adopted from Choi et al. (2018). A three-item scale was adopted from Aïmeur et al. (2016) for measuring privacy data control and the disclosure intention was measured using the scale adopted from Zhu et al. (2021) with some modifications.

Table 1: Measures

Construct	Source	Items
Privacy Fatigue	Choi et al., 2018	1. Dealing with privacy in the Menstrual tracking app is exhausting 2. I'm not in a good mood when I'm dealing with the privacy issues in the Menstrual tracking app 3. I'm not so interested in the privacy issues of the Menstrual tracking app 4. I have doubts about the significance of privacy in the Menstrual tracking app
User Comprehension	Aïmeur et al., 2016	1. The content of this policy makes sense to me. 2. Important information is easily identifiable. 3. I understand all the issues related to my privacy
Disclosure Intention	Zhu et al., 2021	1. In order to use the services of the Menstrual tracking app, I would like to disclose relevant data 2. In order to use the service of the Menstrual tracking app, I will probably disclose relevant information 3. In order to use the services of the Menstrual tracking app, I tend to provide relevant data

Construct	Source	Items
Privacy Data Control	Aïmeur et al., 2016	1. I know that my private data will not be disclosed to a third party without my permission. 2. I can decide who has access to my private data. 3. I can change my mind about my privacy settings whenever I want

Common Method Bias

Due to the same measurement environment, source, and context, we tested for common method variance. As a result of applying Harman's single-factor method to address this concern, the five constructs have a variance of 48.84%, which is below the threshold of 50% (Podsakoff et al., 2003), suggesting that common method variance is absent and does not affect the robustness of results significantly.

Data Analysis

As we used a non-probability sampling technique, the gathered data was not normally distributed. Hence, we opted for Partial Least Square-Structural Equation Modelling (PLS-SEM) with SmartPLS 4.0 to test the hypotheses. Although PLS-SEM provides similar results to its parametric alternative, Covariance Based-SEM, PLS-SEM does not require the data to follow a normal distribution (Dash & Paul, 2021).

Assessment of Measurement Model

Smart PLS 4.0 was employed to find out the result of assumption testing. A consistent PLS algorithm was carried to find the results of reliability analysis, discriminant validity and the VIF values. Based on the results presented in Table 2, Cronbach's alpha ranged from 0.759 to 0.936, and composite reliability ranged from 0.856 to 0.951, both above the benchmark value of 0.7 (Sarstedt et al., 2022). Furthermore, the average variance extracted (AVE) values were higher than the benchmark value of 0.5 (Sarstedt et al., 2022). The measurement model was found to possess good convergent validity and reliability. A discriminant validity test was also conducted using the HTMT criterion, as shown in Table 3, where it can be seen that the value is within the threshold value of 0.90 (Teo et al., 2008). These results demonstrate that the measurement model has satisfactory results.

Table 2: Results of Reliability Analysis

Construct	Number of items	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
DI	3	0.759	0.856	0.669
PDC	3	0.906	0.941	0.842
PF	4	0.823	0.883	0.657
COMP	3	0.936	0.951	0.797

Note: DI=Disclosure Intention, PDC=Privacy Data Control, PF=Privacy Fatigue, COMP=Comprehension

Table 3: HTMT Ratio Results

Construct	Comprehension	Disclosure Intention	Privacy Data Control
Disclosure Intention	0.636		
Privacy Data Control	0.899	0.665	
Privacy Fatigue	0.801	0.555	0.595

Assessment of Structural Model

The structural model results were obtained through SMART PLS 4.0 software, and the results show that the model has a good fit (SRMR= 0.058 and NFI= 0.88). The R square ranged found to be ranging from 0.38 to 0.64, and the Q square ranged from 0.376 to 0.635. F^2 effect size statistic specifies if the removal of an independent variable from the model can have a substantial impact on the dependent variable (Hair et al, 2011). The analysis results of F^2 statistics show that in the context of the present study, a small effect of 0.052 and 0.026 for the dependent variable which is disclosure intention (see Table 4).

Table 4: F^2 Results

Relationships	F^2
Comprehension → Disclosure Intention	0.011
Comprehension → Privacy Fatigue	1.068
Comprehension → Privacy Data Control	2.181
Privacy Fatigue → Disclosure Intention	0.026
Privacy Data Control → Disclosure Intention	0.052

The bootstrapping method (N = 5000) was used to test the paths stated in the hypotheses and the results are presented in Figure 2. The results show that comprehension (β = 0.183, t = 1.353, p > 0.01) has an insignificant impact on disclosure intention, thus, H_1 is rejected. However, users' comprehension of privacy policy has a negative impact on privacy fatigue (β = -0.719, t = 22.315, p < 0.01) and, has a positive impact on privacy data control (β = 0.828, t = 36.272, p < 0.01), hence, H_2 and H_4 are supported. Privacy fatigue was found to have a significant but negative impact on the disclosure (β = -0.184, t = 2.804, p < 0.01) and privacy data control (β = 0.322, t = 3.07, p < 0.01) have a positive impact on disclosure intention. Thus, H_3 is not supported (since it was hypothesised that privacy fatigue would have a positive impact on disclosure intention) while H_5 is supported (see Table 5).

Figure 2: PLS-SEM Path Diagram

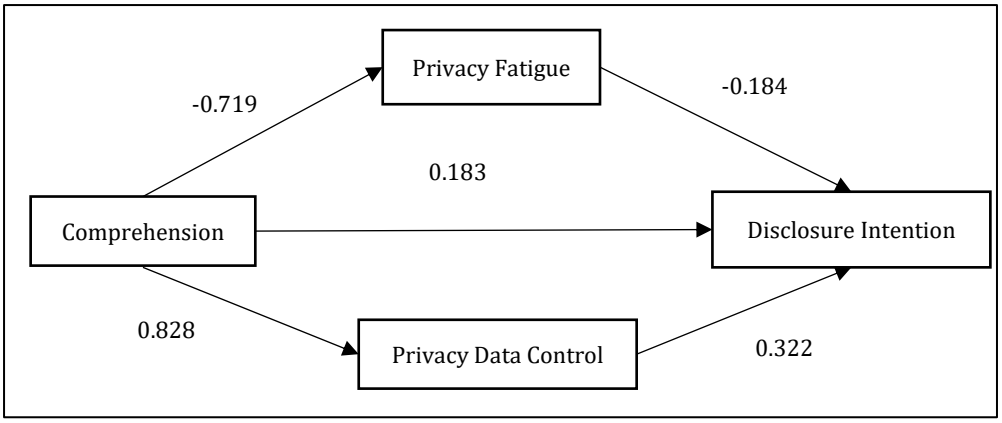


Table 5: Results of Hypothesis Tests

Path	Original Sample	Sample Mean	Standard Deviation	*t*	*p*	Decision
H_1: Comprehension → Disclosure Intention	0.183	0.165	0.135	1.353	0.177	Not Supported
H_2: Comprehension → Privacy Fatigue	-0.719	-0.719	0.032	22.315	0.00	Supported
H_3: Privacy Fatigue → Disclosure Intention	-0.184	-0.193	0.066	2.804	0.005	Not Supported

Path	Original Sample	Sample Mean	Standard Deviation	*t*	*p*	Decision
H_4: Comprehension → Privacy Data Control	0.828	0.829	0.023	36.272	0.00	Supported
H_5: Privacy Data Control → Disclosure Intention	0.322	0.335	0.105	3.07	0.002	Supported

Structural Model Assessment for Indirect Effect (Mediating Effect)

Privacy fatigue and privacy data control play an intermediary role in the relationship between user comprehension of privacy policies, and disclosure intention. Considering that the sample data do not meet the requirements of a normal distribution and the data size is relatively small, we used the bootstrapping method (N = 5000) for the test (Carrión et al., 2017). The results are shown in Table 3. In this study, there are two mediation paths, COMP→PF→DI and COMP→PDC→DI. The direct effect of comprehension of privacy policies on the disclosure intention was found to be insignificant. Both the indirect effects were found to be significant which indicates a case of indirect –only mediation (Zhao et al., 2010) since there exists an indirect effect, but the direct effect of comprehension of privacy policies on the disclosure intention does not exist. This indicates that privacy policy comprehension impacts disclosure intention only indirectly through privacy fatigue and privacy data control (Zhao et al., 2010).

Table 6: Results of the Mediation Effects

Path	Direct Effect	Specific Indirect Effect	Total Indirect Effect	Total Effect	Type of mediation
Comprehension → Privacy Fatigue → Disclosure Intention	0.183 (Insig.)	0.132*	0.399*	0.582*	Indirect only
Comprehension → Privacy Data Control → Disclosure Intention	0.183 (Insig.)	0.267 *	0.399*	0.582*	Indirect only

Note: *$p < 0.001$; Insig. – Insignificant

Discussion

In summary, some interesting results can be gleaned from this study. Even though the study's subject of interest was menstrual tracking applications, the key findings could be generalised to mHealth apps since the nature of data collected is similar. According to the study, the first finding is that users understanding of privacy policies plays a key role in their decision to disclose their information though there is no direct impact. According to the study, ease of comprehension of privacy policies contribute to share personal information only indirectly through privacy data control and privacy fatigue. These findings can be discussed in relation to previous research as follows.

Second, the results provide the answer to one of the research questions, namely, whether there exists a parallel mediation path and which path is stronger. The stronger mediation path is the path where privacy data control exerts a stronger positive impact on the disclosure intention than the privacy fatigue ($|\beta 1| = 0.267 > |\beta 2| = 0.132$). That is, the impact of privacy policy comprehension on greater privacy control leads to a greater disclosure intention in this study. The respondents in this study were given the option to opt-out as a part of the privacy policy, which entails collecting and processing personal data until the user takes affirmative action to opt-out (Degryse & Bouckaert, 2006). Another way of expressing it is that users are given greater control over their data through the privacy policy. This ability to control their private data which is clearly communicated in the policy appears to be the most critical factor that influences their trust in menstrual tracking applications (Aïmeur et al., 2016). Users' ability to understand how their data is used and consent explicitly asked for in the policy (Aïmeur et al., 2016; Degryse & Bouckaert, 2006), thus appears to lead to a greater willingness to disclose information.

Third, in the present study, it could be observed that privacy fatigue has a negative impact on the disclosure intention of the menstrual tracking app users which is opposite to the hypothesis stated. According to some past literature, privacy fatigue positively impacts privacy disclosure intentions (Choi et al., 2018; Zhu et al., 2021) because fatigue reduces people's willingness to spend time and energy on managing private data (Choi et al., 2018). Our findings contradict with the past literature (Choi et al., 2018; Tang et al., 2020; Zhu et al., 2021;) where privacy fatigue was found to have a positive impact on the users' disclosure intention, while in the present study, privacy fatigue was found to have a negative impact on the users' disclosure intention. The reason could be the nature of the menstrual tracking app which requires very intimate information from the users because of which users tend to be more cautious in disclosing information (Fowler et al., 2020).

Theoretical Implications

This study makes several theoretical contributions. First, it widens the research in the users privacy decision making regarding information disclosure in the area menstrual tracking applications. There are few empirical studies pertaining to this area where the impact of privacy policy comprehension on the disclosure intention are analysed. Since menstruation-tracking app is unique among other apps because it is intimate in nature, misalignment between actual and intended use can occur due to an inability to communicate relevant terms (Fowler et al., 2020). This highlights the importance of this study. Second, the study incorporated an opt-out option in privacy policy of the scenario provided to the participants and used privacy data control as a mediating variable. The results have indicated the stronger mediating effect of data control on the disclosure intention in the FemTech apps. It is possible that when the users were given an opt-out option, they perceived themselves to be more capable of controlling their own information, thus suggesting it to be a correct addition to the privacy policies of FemTech apps as stated in the privacy data control literature (Degryse & Bouckaert, 2006).

Managerial Implications

This study entails certain implications for mobile health application providers. First, as the perception of users regarding privacy data control can be enhanced by implementing a highly comprehensible privacy policy, operators and designers should focus on privacy policies easier to understand (Aïmeur et al., 2016). The present study's findings will encourage the providers of mHealth applications to implement a clear and easy-to-read format to make privacy policies easily understandable to users. Using openness and transparency as the basis for their applications, they should consider improving readability, simplicity, and humanisation (Aïmeur et al., 2016; Degryse & Bouckaert, 2006). This will increase the users sense of privacy data control, and thereby, their willingness to disclose information. Secondly, operators and designers should consider providing a broader range of service function setting permissions that cover the privacy control needs of users as well (Degryse & Bouckaert, 2006). Users will perceive significant benefits from a privacy function that gives them control (Guo et al., 2022). Users daily use of the application could also be taken into account when determining privacy settings (Aïmeur et al., 2016; Guo et al., 2022).

The area of mHealth applications is plagued by privacy fatigue (Zhu et al., 2021). One way in which privacy fatigue may contribute to user disclosure is that it increases the risk of user disclosure of their health information (Fowler et al., 2020; Zhu et al., 2021) Our study findings signify that privacy fatigue has a detrimental impact on the

disclosure intention of the users, which contradicts past literature (Choi et al., 2018; Zhu et al., 2021, Tang et al., 2020). As noted previously, this could be because apps such as the menstrual tracking app require very intimate information of the users. Thus, developers of mHealth apps that use highly sensitive personal data should be extra careful in clearly explaining their privacy policies.

Conclusion

This study took into consideration the menstrual tacking applications which deals with data of sensitive nature and their diverse uses which can generate several risks. Privacy policy plays a critical role in this type of health app because it is the channel through which the users put their trust in the app providers and disclose their personal information in return for the service promised by the application. A privacy policy which can easily be comprehended by users and instils the trust of users on the app, will eventually lead to the development of the FemTech industry. The rise of FemTech industry could contribute to women empowerment. Simple and efficient solutions are required for menstrual tracking app users to regain their trust after privacy fatigue. It has been recommended that policies should be simplified, smart contracts should be applied to policy formulation, and technologies should be introduced to protect users' anonymity while sharing personal data are some solutions to the paradox of privacy fatigue. Providing more flexibility in their privacy policies and giving users more control over their data is the right way to improve privacy. Thus, a privacy policy with an easily comprehensible content and the power given to the users to have a control over their data while using the menstrual tracking app could be a game-changer in the FemTech industry.

Scope for Future Research

This study adopts a scenario-based questionnaire for the data collected and is a cross-sectional study. It could also be carried with the help of a quasi-experimental research design, especially with the use of data control mechanisms such as opt-out options. Here, the disclosure intention is being studied, future studies could study the actual behaviour which could provide some interesting observations. Future studies could also consider the impact of personality traits and factors related to technology users' privacy decision-making paths, since the mobile health industry is gradually developing and evolving.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

References:

Aïmeur, E., & Lafond, M. (2013). The scourge of internet personal data collection. 2013. *International Conference on Availability, Reliability and Security* (pp. 821–828). IEEE. https://doi.org/10.1109/ARES.2013.110

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, *58*, 368–379. https://doi.org/10.1016/j.chb.2015.11.014

Angulo, J., Fischer-Hübner, S., Wästlund, E., & Pulls, T. (2012). Towards usable privacy policy display and management. *Information Management & Computer Security*, *20*(1), 4–17. https://doi.org/10.1108/09685221211219155

Awad, N. F., & Krishnan, M. S. (2006). The Personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28. https://doi.org/10.2307/25148715

Bansal, S. (2021). Femtech Mobile Apps- Digitizing Women's Healthcare. *Dew Solutions*. https://www.dewsolutions.in/femtech-mobile-apps/

Cakebread, C. (2017, November 15). You're not alone, no one reads terms of service agreements. Business Insider. https://www.businessinsider.in/youre-not-alone-no-one-reads-terms-of-service-agreements/articleshow/61659553.cms

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24–31. https://doi.org/10.1016/j.csi.2015.04.001

Caramujo, J., & Da Silva, A. M. R. (2015). Analyzing privacy policies based on a privacy-aware profile: The facebook and linkedIn case studies. (2015). *17th Conference on Business Informatics* (pp 77–84). IEEE. https://doi.org/10.1109/CBI.2015.44

Carrión, G. C., Nitzl, C., & Roldán, J. L. (2017). Mediation analyses in partial least squares structural equation modeling: Guidelines and empirical examples. In H. Latan & R. Noonan (Eds.), *Partial least squares path modeling* (pp. 173–195). Springer International Publishing. https://doi.org/10.1007/978-3-319-64069-3_8

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Cooper-Martin, E. (1993). Effects of information format and similarity among alternatives on consumer choice processes. *Journal of the Academy of Marketing Science*, *21*, 239–246. https://doi.org/10.1177/0092070393213007

Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, *173*, 121092. https://doi.org/10.1016/j.techfore.2021.121092

Degryse, H., & Bouckaert, J. (2006). *Opt in versus opt out: A free-entry analysis of privacy policies* (Working Paper No. 1831). SSRN. https://doi.org/10.2139/ssrn.939511

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, *52*(2), 227–237. https://doi.org/10.1109/TEM.2005.844927

Ermakova, T., Fabian, B., & Babina, E. (2015). Readability of privacy policies of healthcare websites. *12th International Conference on Wirtschaftsinformatik*.

Fowler, L. R., Gillard, C., & Morain, S. R. (2020). Readability and accessibility of terms of service and privacy policies for menstruation-tracking smartphone applications. *Health Promotion Practice*, *21*(5), 679–683. https://doi.org/10.1177/1524839919899924

Furnell, S., & Phippen, A. (2012). Online privacy: A matter of policy? *Computer Fraud & Security*, *2012*(8), 12–18. https://doi.org/10.1016/S1361-3723(12)70083-0

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), 33–43. https://doi.org/10.1016/j.jsis.2014.09.001

Goodhue, D. L, Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*, *36*(3), 981–1001. https://doi.org/10.2307/41703490

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: The role of vulnerability, benevolence and privacy concern. *Journal of Enterprise Information Management*, *35*(3), 774–795. https://doi.org/10.1108/JEIM-12-2020-0481

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. https://ijoc.org/index.php/ijoc/article/viewFile/4655/1738

Hoffmann, A., Waubert de Puiseau, B., Schmidt, A. F., & Musch, J. (2017). On the comprehensibility and perceived privacy protection of indirect questioning

techniques. *Behavior Research Methods*, *49*, 1470–1483. https://doi.org/10.3758/s13428-016-0804-3

Keith, M. J., Maynes, C., Lowry, P. B. and Babb, J. (2014). Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. *International Conference on Information Systems (ICIS 2014)*, Auckland, (pp. 14–17).

Lee, J.-M., & Rha, J.-Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, *63*, 453-462. https://doi.org/10.1016/j.chb.2016.05.056

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. https://doi.org/10.1016/j.dss.2011.01.017

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Maslach, C. (2001). What have we learned about burnout and health? *Psychology & Health*, *16*(5), 607–611. https://doi.org/10.1080/08870440108405530

Medine, D., & Murthy, G. (2019). Nobody reads privacy policies: Why we need to go beyond consent to ensure data privacy. Next Billion. https://nextbillion.net/beyond-consent-for-data-privacy/

Mehrnezhad, M., Shipp, L., Almeida, T., & Toreini, E. (2022, September). Vision: Too little too late? do the risks of FemTech already outweigh the benefits?. In *Proceedings of the 2022 European Symposium on Usable Security* (pp. 145-150). https://dl.acm.org/doi/pdf/10.1145/3549015.3554204

Mishra, S. (2015, September 17). New report finds more than 165,000 mobile health apps now available, takes close look at characteristics & use. IMedicalApps. https://www.imedicalapps.com/2015/09/ims-health-apps-report/

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs*, *36*(1), 28–49. https://doi.org/10.1111/j.1745-6606.2002.tb00419.x

Narayan, A. (2022, August 3). Period Tracking applications and privacy: How safe is it to share intimate details on these apps? Feminism in India. https://feminisminindia.com/2022/08/03/period-tracking-applications-privacy-safety-intimate-details-apps/

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, *4*(3), 1–14. https://doi.org/10.1177/2056305118784770

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management*, *30*(6), 467–480. https://doi.org/10.1016/j.jom.2012.06.002

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://www.iges.or.jp/system/files/publication_documents/pub/peer/10694/21baae66a93e9c7e5b3cbce0dbc6ffbc70c2.pdf

Rotenberg, M., & Jacobs, D. (2013). Updating the law of information privacy: The new framework of the European Union. *Harvard Journal of Law and Public Policy*, *36*(2), 605.

Sarstedt, M., Hair, J. F., Pick, M., Liengaard, B. D., Radomir, L., & Ringle, C. M. (2022). Progress in partial least squares structural equation modeling use in marketing research in the last decade. *Psychology & Marketing*, *39*(5), 1035–1064. https://doi.org/10.1002/mar.21640

Schomakers, E.-M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, *46*, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Siapka, A., & Biasin, E. (2021). Bleeding data: The case of fertility and menstruation tracking apps. *Internet Policy Review*, *10*(4), 1–34. https://doi.org/10.14763/2021.4.1599

Strachan, S. M., Brawley, L. R., Spink, K. S., & Jung, M. E. (2009). Strength of exercise identity and identity-exercise consistency: Affective and social cognitive relationships. *Journal of Health Psychology*, *14*(8), 1196–1206. https://doi.org/10.1177/1359105309346340

Tang, J., Akram, U., & Shi, W. (2020). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management*, *34*(4), 1097–1120. https://doi.org/10.1108/jeim-03-2020-0088

Teo, T. S. H., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems*, *25*(3), 99–132. https://doi.org/10.2753/MIS0742-1222250303

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018, April). I read but don't agree: Privacy policy benchmarking using machine learning and the EU GDPR. *Companion Proceedings of the Web Conference 2018* (pp. 163–166). https://doi.org/10.1145/3184558.3186969

Wadhwa, R., & Bains, G. (2022). The evolution of India's data privacy regime in 2021. iapp. https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/

Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Giovanni Leon, P., Schaarup Andersen, M., Zimmeck, S., Sathyendra, K. M., Russell, N. C., B. Norton, T., Hovy, E., Reidenberg, J., & Sadeh, N. (2016). The creation and analysis of a website privacy policy corpus. *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics* (Volume 1: Long Papers), 1330–1340. https://doi.org/10.18653/v1/P16-1126

Wolford, B. (2018, November 7). What is GDPR, the EU's new data protection law? GDPR.Eu. https://gdpr.eu/what-is-gdpr/

Xie, E., Teo, H.-H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, *17*, 61–74. https://doi.org/10.1007/s11002-006-4147-1

Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, *124*, 667–675. https://doi.org/10.1016/j.jbusres.2020.02.006

Zhao, X., Lynch, J. G., Jr., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206. https://doi.org/10.1086/651257

Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, *54*(4), 427–437. https://doi.org/10.1016/j.im.2016.10.001

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

Zolkepli, I. A., Mukhiar, S. N. S., & Tan, C. (2021). Mobile consumer behaviour on apps usage: The effects of perceived values, rating, and cost. *Journal of Marketing Communications*, *27*(6), 571–593. https://doi.org/10.1080/13527266.2020.1749108

Appendix

The Scenario

Flo is a menstrual tracking app which is on a mission to build a better future for female health. This app also wants to build a better and more inclusive future for all people who

menstruate. Its AI-powered tech, personalised insights and tailored support helps the users feel more in control every day.

Since it is a mHealth app, it collects information such as

- Name
- Email address
- Year of birth
- Password or passcode
- Place of residence and associated location information including time zone and language
- ID (for limited purposes)

When you sign up to use the services, you may choose to provide personal data about your health and well-being such as:

- Weight
- Body temperature
- Menstrual cycle dates
- Details of your pregnancy (if you select the pregnancy mode)
- Various symptoms related to your menstrual cycle, pregnancy and health
- Other information about your health (including sexual activities), physical and mental well-being, and related activities, including personal life.

How We Use Your Personal Data

We will not collect and use your personal data without letting you know. Depending on which features of the services you use, we will process your personal data based on one or more of the following legal bases:

1. **Your consent.** For example, on the registration screen when you give us permission to process your Personal Data.
2. **To fulfill our contractual obligations to you in order to provide the Services to you.**
3. **Legitimate interest.** We may process your Personal Data in relation to our interests in providing the Services to you, our commercial interests, including our interest in protecting the security and integrity of the Services, and wider societal benefits.
4. **Legal obligation.** We may be obligated to process some of your Personal Data to comply with applicable laws and regulations.

- I agree
- I do not agree
- I wish my personal data to be collected only when I give my explicit agreement and only to be used for my service

Since our private data is taken into consideration, privacy portal or policy plays an important role. Above was an excerpt of the privacy policy of the Flo app and below is the image of the privacy portal of the Flo app.