

Summer 6-30-2018

A Personalization-Privacy Paradox in Usage of Mobile Health Services: A Game Theoretic Perspective

Fanbo Meng

School of Management, Harbin Institute of Technology, Harbin, China; Faculty of Business, The Hong Kong Polytechnic University, Kowloon, Hong Kong.

Xitong Guo

School of Management, Harbin Institute of Technology, Harbin, China.

Kee-hung Lai

Faculty of Business, The Hong Kong Polytechnic University, Kowloon, Hong Kong.

Xinli Zhao

School of Management, Harbin Institute of Technology, Harbin, China

Follow this and additional works at: <http://aisel.aisnet.org/whiceb2018>

Recommended Citation

Meng, Fanbo; Guo, Xitong; Lai, Kee-hung; and Zhao, Xinli, "A Personalization-Privacy Paradox in Usage of Mobile Health Services: A Game Theoretic Perspective" (2018). *WHICEB 2018 Proceedings*. 18.
<http://aisel.aisnet.org/whiceb2018/18>

This material is brought to you by the Wuhan International Conference on e-Business at AIS Electronic Library (AISeL). It has been accepted for inclusion in WHICEB 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Personalization-Privacy Paradox in Usage of Mobile Health

Services: A Game Theoretic Perspective

Fanbo Meng^{1,2}, Xitong Guo^{1}, Kee-hung Lai², and Xinli Zhao¹*

¹School of Management, Harbin Institute of Technology, Harbin, China.

²Faculty of Business, The Hong Kong Polytechnic University, Kowloon, Hong Kong.

Abstract: As health information privacy concern of the public raises, people are hesitant on disclosure of their private health information for personalized health services from using mobile health. The tension between personalization and privacy hinders users' adoption of mobile health services. In this study, we draw on game theory to explain the personalization-privacy paradox in the usage of mobile health services. The results show that: (1) In a one-shot game, the strategy set of mobile health marketers and users will be contrary to their original motivations. (2) In a repeated game, collecting users' private health information in a friendly way and disclosing private health information will be dominant strategies for both players. Managers need to pay attention to these scenarios in promoting usage of mobile health services.

Keywords: game theory, mHealth, personalization, privacy concern, technology acceptance

1. INTRODUCTION

As the mobile information communication technology evolves, the usage of mobile devices for accessing personalized healthcare services has dramatically increased ^[1]. Mobile health (mHealth) can capture users' health information and preferences in digital format and suggest corresponding individual-tailored health services to users. Using mHealth services will bring benefits to users including personalized health information, lower healthcare costs, improved medical outcomes, a more effective health services process, and a more efficient personal health data management ^[2]. Due to the capable features of mobile information communication technology, such as Global Position System (GPS) and sensors, the mHealth service providers or marketers can easily collect individuals' real-time health data including walking steps, heart rate, and blood pressure through their mobile device. To seek personalized health services and consult health professionals through mobile platforms, users are required to upload or report their health records, medical histories, demographic characteristics, and contact numbers, and so forth onto the platform. Based on real-time and self-reported health information, the service providers command a better position to understand users' health needs and hence provide customized health services. Despite the popularity of personalized health services, they are reluctant to report and disclose their private health-related information and data to mHealth marketers in view of the growing privacy concern in recent years. Such dilemma can be considered as a personalization-privacy paradox ^[3], suggesting "the tension between how the developers and marketers of IT applications exploit users' information to offer them personalized services, and those users' growing concerns about the privacy of that information, which can restrain their use of such applications" ^[4]. In the management information systems (MIS) literature, individuals' intentions to adopt a new technology is promoted by personalization but discouraged by privacy concern. Recent empirical studies highlight such personalization-privacy paradox in the use of online personalized services ^[5], electronic health records (EHRs) ^[6], smartphone ^[4], and mHealth services ^[7].

One novel aspect of this study is to use the game theory to explain the role of personalization-privacy

paradox in the adoption of mHealth services. From the game-theoretical perspective, mobile health users and mobile health marketers can be regarded two game players. The strategy set of mobile health marketers includes a friendly way and a hostile way to collect private health information, respectively. The former requires mobile health marketers to collect and analyze users' private health information in a friendly way, offering them personalized health information and services based on users' private health information. The latter performs such activities in a hostile way with the intention to abuse or disclose users' private health information for illegal profit-making. The strategy set of mobile health users includes 1) disclosing or 2) protecting personal private health information. In the first one, mobile health users allow mobile health marketers to collect their private health information and enjoy personalized health information and services in return for health care. Alternatively, they refuse to share their private health information with mobile health marketers, keeping their private health information safe under the second strategy.

Payoff functions of this game present the profits and losses of two players. The losses and payoffs of two players' strategic actions are significant determinants of their decision-making. Based on the game-theoretic perspective, this study aims to investigate how to reduce users' health privacy concern and leverage the power of personalization in promoting the usage of mobile health services.

In a two player game, mobile health users will make a response according to the strategies of mobile health marketers. To maximize payoffs, mobile health marketers' dominant strategy is to collect users' private health information in a hostile way when users choose to disclose their private health information. Therefore, based on the marketers' strategy, users are reluctant to share their private health information because the latter worried about unintentional disclosure of their private health information or even abuse for illegal profit-making. While this strategy set could partially explain the personalization-privacy paradox, yet this result may be only applied in the context of a one-shot game. Indeed, many mobile health marketers prefer a long-term relationship with their users for maximum profit rather than a one-shot game. Although mobile health users have a concern about their health privacy, they are keen on personalized health services. Strategies of two players in a long-term relationship may differ from those of a one-shot game. To better explain the personalization-privacy paradox in mHealth context, we discuss both players' strategies and payoffs from perspectives of both a one-shot game and a repeated game.

In this study, we follow two rules: 1) different users have different tolerance levels in private health information disclosure; 2) the possibility of users' private health information disclosure will increase if mobile health marketers frequently come to collect users' private health information. Therefore, we assume that the way marketers collecting users' private health information under users' tolerance level is seen as a friendly way, however, the way of collecting users' private health information beyond users' tolerance level is seen as a hostile way. Obviously, different strategies of two players will bring different payoffs and losses to each other. Both players will take into consideration their prior beliefs in evaluating payoffs and losses in the game. Therefore, a repeated game theory may be appropriate to explain this process, and Nash equilibrium may exist in this game.

The remainder of this paper proceeds as follows. In the next section, we discuss strategies and payoffs of mobile health marketers and users in a one-shot game. Next, we describe strategies and payoffs of two players respectively in a repeated game. We conclude with a description of our results and implications for research and practice.

2. STRATEGIES AND PAYOFFS OF TWO PLAYERS IN A ONE-SHOT GAME

In this game, two game players include private health information marketers and mobile health users. We discuss their different strategies and payoffs when using different strategies in this game respectively.

U_{profit}^{dis} refers to the profit that mobile health users gained when mobile health marketers take the

strategy of collecting users’ private health information in a friendly way, and mobile health users take the strategy of disclosing their private health information. This also refers to the profit mobile health users lost when mobile health marketers take the strategy of collecting users’ private health information in a friendly way, however, mobile health users are reluctant to disclose their private health information. This profit indicates that mobile health users could gain personalized health information and services to better serve their health needs.

$M_profit_{fri}^{dis}$ refers to the profit mobile health marketers gained when mobile health marketers choose to collect users’ private health information in a friendly way, while users allow marketers to collect their private health information from them. This profit means that mobile health marketers could better understand users’ specific health need and design mobile health services through collecting and analyzing users’ private health information.

$U_loss_{hos}^{dis}$ refers to the loss mobile health users suffered when mobile health marketers choose to collect users’ private health information in a hostile way, while users allow marketers to collect their health information. The loss is that mobile health users’ private health information is abused and leaked out for illegal profit-making by mobile health marketers.

$M_income_{hos}^{dis}$ refers to the profit mobile health marketers gained when mobile health marketers take the strategy of collecting users’ private health information in a hostile way, while mobile health users choose to disclose their private health information. This profit is different from the profit gained through collecting private health information in a friendly way. Although mobile health marketers may undertake higher risk, they can gain a higher profit from this strategy of collecting users’ private health information in a hostile way.

$U_income_{hos}^{pro}$ refers to the profit mobile health users gained when mobile health marketers collect users’ private health information in a hostile way, while mobile health users refuse to share their private health information with marketers. These profits indicate that mobile health users protect their health privacy and avoid the risk that they may suffer from private health information disclosure and abuse.

Based on the above analysis, both game players should choose following strategies: collecting private health information in a friendly way and disclosing private health information respectively, in order to gain profits and nurture a trusting relationship. When two players choose strategy set: collecting private health information a hostile way and disclosing private health information respectively, mobile health marketers could gain higher payoffs while mobile health users suffer losses in this game. When both game players choose strategy set: collecting private health information in a friendly way and protecting private health information respectively, mobile health marketers could not gain any profit and mobile health users miss the opportunity to enjoy personalized health information and services. When both game players choose strategy set: collecting health information in a hostile way and protecting private health information respectively, mobile health marketers could not gain any profit in this process, however, mobile health users prevent their private health information from private health information abuse. This game matrix is presented in Table 1.

Table 1 Game Matrix in a One-shot Game

Mobile Health Users	Mobile Health Marketers	
	Friendly	Hostile
Disclose	$U_profit_{fri}^{dis}, M_profit_{fri}^{dis}$	$-U_loss_{hos}^{dis}, M_profit_{hos}^{dis}$
Protect	$-U_profit_{fri}^{dis}, 0$	$U_profit_{hos}^{pro}, 0$

From the perspective of mobile health marketers, when mobile health users choose the strategy of disclosing private health information, the dominant strategy of mobile health marketers is to collect private health information in a hostile way. That is $M_profit_{hos}^{dis} > M_profit_{fri}^{dis}$. When mobile health users choose the strategy of protecting their private health information, the profit for mobile health marketers will be 0. From the

perspective of mobile health users, when mobile health marketers choose the strategy of collecting private health information in a friendly way, the dominant strategy of mobile health users is disclosing private health information. That is $U_profit_{fri}^{dis} > -U_profit_{fri}^{dis}$. When mobile health marketers choose the strategy of collecting private health information in a hostile way, the dominant strategy of mobile health users is protecting their private health information. That is $U_profit_{hos}^{pro} > -U_loss_{hos}^{dis}$. Based on the above strategies, there is a pure strategy Nash equilibrium $(U_profit_{hos}^{pro}, 0)$ in this game matrix. However, in fact, both mobile health marketers and users aim to communicate and share information through this emerging platform in a long term. Therefore, both marketers and users may not actually have the outcome reaching this Nash equilibrium. Although users may face the risk of privacy disclosure or abuse, they still choose to share their private health information in order to get better-personalized health information and services. To get continued profit, mobile marketers may change their strategies for longer-term customer relationship development. The dominant strategy of this game may be contrary to both players' original motivations. Therefore, this echoes a prisoner's dilemma between mobile health marketers and users which is discussed in a repeated game context below.

3. STRATEGIES AND PAYOFFS OF TWO PLAYERS IN A REPEATED GAME

Further to a one-shot game, we draw on a repeated game to discuss the prisoners' dilemma between mobile health marketers and mobile health users. Strategy sets of both players are a finite set. Then, in this repeated game process, the payoff of each strategy of mobile health marketers and mobile health users will be discussed as follows. δ refers to a discount factor of mobile health users' future payoff and ζ refers to a discount factor of mobile health marketers' future payoff.

From the perspective of mobile health users, when mobile health marketers collect private health information from users in a friendly way, users can choose to disclose their private health information or not. In this context, the payoff of users will be presented as $u_profit_{fri}^{dis}$. Therefore, when mobile health marketers collect users' private health information at the n^{th} time, mobile health users' payoff is $U^r_profit_{fri}^{dis}$.

$$U^r_profit_{fri}^{dis} = u_profit_{fri}^{dis} + u_profit_{fri}^{dis} * \delta + u_profit_{fri}^{dis} * \delta^2 + \dots + u_profit_{fri}^{dis} * \delta^n = u_profit_{fri}^{dis} * \frac{1 - \delta^n}{1 - \delta}$$

When mobile health marketers collect users' private health information in a hostile way, mobile health users choose to disclose their private health information. In this context, the payoff of users will be presented as $u_loss_{hos}^{dis}$. Therefore, when mobile health marketers collect users' private health information at the n^{th} time, mobile health users' payoff is $U^r_loss_{hos}^{dis}$.

$$U^r_loss_{hos}^{dis} = u_loss_{hos}^{dis} + u_loss_{hos}^{dis} * \delta + u_loss_{hos}^{dis} * \delta^2 + \dots + u_loss_{hos}^{dis} * \delta^n = u_loss_{hos}^{dis} * \delta * \frac{1 - \delta^n}{1 - \delta}$$

When mobile health marketers collect users' private health information in a hostile way, mobile health users choose to protect their private health information. In this context, the payoff of users will be presented as $u_profit_{hos}^{pro}$. Therefore, when mobile health marketers collect users' private health information at the n^{th} time, mobile health users' payoff is $U^r_profit_{hos}^{pro}$.

$$U^r_profit_{hos}^{pro} = u_profit_{hos}^{pro} + u_profit_{hos}^{pro} * \delta + u_profit_{hos}^{pro} * \delta^2 + \dots + u_profit_{hos}^{pro} * \delta^n = u_profit_{hos}^{pro} * \frac{1 - \delta^n}{1 - \delta}$$

From the perspective of mobile health marketers, when marketers choose to collected users' private health information in a friendly way, mobile health users disclose their private health information. In this context, the payoff of marketers will be presented as $m_profit_{fri}^{dis}$. Therefore, when mobile health marketers collect users' private health information at the n^{th} time, mobile health marketers' payoff is $M^r_profit_{fri}^{dis}$.

$$M^r_profit_{fri}^{dis} = m_profit_{fri}^{dis} + m_profit_{fri}^{dis} * \zeta + m_profit_{fri}^{dis} * \zeta^2 + \dots + m_profit_{fri}^{dis} * \zeta^n = m_profit_{fri}^{dis} * \frac{1 - \zeta^n}{1 - \zeta}$$

When mobile health marketers collect users’ private health information in a hostile way, mobile health users choose to disclose their private health information. In this context, the payoff of marketers will be presented as $m_profit_{hos}^{dis}$. Therefore, when mobile health marketers collect users’ private health information at the n^{th} time, mobile health marketers’ payoff is $M^r_profit_{hos}^{dis}$.

$$M^r_profit_{hos}^{dis} = m_profit_{hos}^{dis} + m_profit_{hos}^{dis} * \zeta + m_profit_{hos}^{dis} * \zeta^2 + \dots + m_profit_{hos}^{dis} * \zeta^n = m_profit_{hos}^{dis} * \frac{1 - \zeta^n}{1 - \zeta}$$

When mobile health marketers collect users’ private health information in a hostile way, mobile health users choose to protect their private health information. In this context, the payoff of marketers will be presented as $m_loss_{hos}^{pro}$. Therefore, when mobile health marketers collect users’ private health information at the n^{th} time, mobile health marketers’ payoff is $M^r_loss_{hos}^{pro}$.

$$M^r_loss_{hos}^{pro} = m_loss_{hos}^{pro} + m_loss_{hos}^{pro} * \zeta + m_loss_{hos}^{pro} * \zeta^2 + \dots + m_loss_{hos}^{pro} * \zeta^n = m_loss_{hos}^{pro} * \frac{1 - \zeta^n}{1 - \zeta}$$

Based on the above payoffs and losses of mobile health users and mobile health marketers, the game matrix of two players in this context is listed in Table 2.

Table 2 Game Matrix in a Repeated Game

Mobile Health Users	Mobile Health Marketers	
	Friendly	Hostile
Disclose	$U^r_profit_{fri}^{dis}, M^r_profit_{fri}^{dis}$	$-U^r_loss_{hos}^{dis}, M^r_profit_{hos}^{dis}$
Protect	$-U^r_profit_{fri}^{dis}, 0$	$U^r_profit_{hos}^{pro}, -M^r_loss_{hos}^{pro}$

Under this repeated game, when mobile health users’ strategy is to disclose their private health information, the dominant strategy for mobile health marketers is to collect users’ private health information in a hostile way rather than collecting data in a friendly way. Therefore, we can have that $M^r_profit_{hos}^{dis} > M^r_profit_{fri}^{dis}$. When mobile health users’ strategy is to protect their private health information, the dominant strategy for mobile health marketers is to collect users’ private health information in a friendly way. Accordingly, we can have $-M^r_loss_{hos}^{pro} < 0$. From the perspective of mobile health users, when marketers’ strategy is to collect private health information in a friendly way, disclosing private health information is profitable for users. Therefore, we can have that $U^r_profit_{fri}^{dis} > -U^r_profit_{fri}^{dis}$. When marketers’ strategy is to collect private health information in a hostile way, protecting private health information is profitable for users. Accordingly, we can have that $U^r_profit_{hos}^{pro} > -U^r_loss_{hos}^{dis}$.

Based on the above statements, in this repeated game context, we could easily find the dominant strategy for two game players. From the perspective of mobile health marketers, we can see that

$M^r_profit_{hos}^{dis} > M^r_profit_{fri}^{dis} > 0 > -M^r_loss_{hos}^{pro}$. In this case, collecting users’ private health information in a hostile way will lead to loss rather than 0, when mobile health users’ strategy is to protect their private health information. In a long-term, therefore, collecting users’ private health information in a friendly way is continuously profitable for marketers. From the perspective of mobile health users, we can see that $U^r_profit_{fri}^{dis} > U^r_profit_{hos}^{pro} > -U^r_loss_{hos}^{dis}$. Therefore, when marketers’ strategy is to collect users’ private health information in a friendly way, the best response strategy of users will be disclosing private health information. When marketers’ strategy is to collect users’ private health information in a hostile way, the best response strategy of users will be protecting their private health information. In this case, marketers will choose to collect users’ private health information in a friendly way for continued profit, and then users will disclose their private health information. Therefore, the best response set for marketers and users will be $(U^r_profit_{fri}^{dis}, M^r_profit_{fri}^{dis})$. This strategy set will lead to mutual benefits for both players in the long run.

4. DISCUSSION AND CONCLUSIONS

In this study, we draw on the game theory to explain the personalization-privacy paradox in the context of mobile health services. Health services, different from other services, is closely related to peoples' lives. Individuals may take cautious attitudes toward this emerging health services from a mobile platform. Users could enjoy personalized health services from mobile platforms, such as smartphones if they agree to upload and report their health record, medical history, and demographic characteristics. However, users are hesitant that mobile health marketers or servers may disclose or abuse their private information for illegal profit-making. With respect to mobile health marketers, in a one-shot game, the dominant strategy of marketers is to collect users' private health information in a hostile way for maximum profit. However, in a repeated game, collecting users' private health information in a friendly way is profitable for the marketer in a long term.

This study contributes to the knowledge stock of mobile health marketers by presenting an insight of the personalization-privacy paradox from game-theoretical perspective. Marketers aim to build a long-term relationship with users in order to continuously collect users' private health information to better understand users' health needs and provide personalized health services to users for profit. To make their payoffs maximum, marketers should choose the strategy of collecting users' private health information in a hostile way in a one-shot game. Instead, marketers choose to collect users' private health information in a friendly way in the repeated game in a long term. In practice, compared to a hostile collection of users' private health information, collecting private health information in a friendly way could not only reduce users' health privacy concern and offer users personalized health services but also avoid network security inspection. For marketers, our recommendations are that they should incorporate privacy-safe features and user-friendly designs in the mobile health application development.

For mobile health users, they hope to gain benefits from personalized health services but are highly concerned about health privacy. In this game, users will choose the best way to respond the strategy of mobile health marketers in order to maximize their own payoff. If mobile health marketers' strategy is to collect users' private health information in a hostile way, users' best response is to protect their private health information. If mobile health marketers' strategy is to collect users' private health information in a friendly way, users' best response is to disclose their private health information. In practice, comparing to protecting private health information, disclosing private health information is beneficial to users who can gain personalized health services, and to marketers who can utilize private health information to generate individually tailored health services for maximum payoff. Our study recommends that users should alleviate their health privacy concerns, and feel more secure that their private health information never actually be abused in a long run.

REFERENCES

- [1] Akter S, D'Ambra J, Ray P. User perceived service quality of m-Health services in developing countries [J]. 18th European Conference on Information Systems, 2010, 1-12.
- [2] Rai A, Chen L, Pye J, et al. Understanding determinants of consumer mobile health usage intentions, assimilation, and channel preferences [J]. *Journal of Medical Internet Research*, 2013, 15(8): e149.
- [3] Awad N F, Krishnan M S. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization [J]. *MIS Quarterly*, 2006, 30(1): 13-28.
- [4] Sutanto J, Palme E, Tan C-H, et al. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users [J]. *MIS Quarterly*, 2013, 37(4): 1141-64.
- [5] Chellappa R K, Sin R G. Personalization versus privacy: An empirical examination of the online consumer's dilemma [J]. *Information Technology and Management*, 2005, 6(2): 181-202.

- [6] Angst C M, Agarwal R. Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion [J]. *MIS Quarterly*, 2009, 33(2): 339-70.
- [7] Guo X, Sun Y, Yan Z, et al. Privacy-Personalization Paradox in Adoption of Mobile Health Service: The Mediating Role of Trust; proceedings of the PACIS, F, 2012 [C].