Dark Pattern: A Serious Game for Learning About the Dangers of Sharing Data

Ingvar Tjostheim[1], Vanessa Ayres-Pereira[2], Chris Wales[3], Angela Manna[4] and Simon Egenfeldt-Nielsen[5,]
[1]DART, Norwegian Computing Center, Oslo, Norway
[2]Department of Psychosocial Science, Faculty of Psychology, University of Bergen, Bergen, Norway
[3]Hauge School of Management, NLA, Oslo, Norway
[4]Serious Games Interactive, Copenhagen, Denmark
ingvar@nr.no
vanessa.aires@uib.no
chris.wales@nla.no
am@seriousgames.net
sen@seriousgames.net

Abstract. Dark patterns refer to tricks built into websites and apps to manipulate users into acting unintentionally and detrimentally. An important issue is how such patterns might affect behaviour when actors are manoeuvred towards the sharing of their personal data, as exemplified in choices we face when downloading Apps or signing up for services provided on the internet. This paper presents our exploratory research into understanding the intention and subsequent actions of older teenagers responding to issues of personal data collection and (mis)use. The research is based on the competitive board-game *Dark Pattern*, in which players install apps, draw dark pattern cards, and make choices about the sharing of personal data. To win the game, a player must share as little data as possible and play cards that punish other players. We were interested to find out the extent to which the game was able to convey types of dark patterns to the players. Additionally, we wanted to explore how players' perceptions of risks in data-sharing associated with their intention to protect their personal data. Finally, we were interested to explore potential gender difference, and whether this might be associated with intention to protect personal data. 56 of the students who played the game answered a subsequent survey with questions about their experiences and the data was analysed using Partial Least Squares – Structural Equation modelling (PLS-SEM). Despite the findings showing that playing the game had only limited impact on knowledge about dark patterns matters, the analysis of the relationship with the factors in our model shows that knowledge has a significant contribution on behavioural intention, demonstrating that students with high dark pattern knowledge also report higher intention to take steps to protect their data.

Keywords: dark patterns, Serious games, learning, user-test, exploratory study, sharing of personal data, personal data security, partial least squares path modelling

1. Introduction

As everyday life becomes increasingly digitized, website and app developers have been collecting considerable amounts of data from internet users. In response to society's concern regarding what seems to be the discreet practice of excessive data collection, general regulations have forced online platforms to implement a notice-and-consent regime. That is, platforms must give users the option to consent or not to the data collection via an active accession, in this case by confirming through a 'click'. The notice-and-consent regime, however, is based on the myth that human decisions are entirely free and rational (Acquisti, 2015) when, in reality, decisions are more greatly constrained by contextual factors. Several online services benefit from this interpretive flaw by implementing so-called Dark Patterns, also known as deceptive design patterns. Dark pattern was a term coined by UX expert Harry Brignull (Brignull et al., 2015) to refer to interface design strategies used by websites and app developers to manipulate or trick internet users into agreeing to disclose their personal information. One of the problems with dark patterns is that, in general, this type of tactic serves the benefit of the online service, rather than the user.

The darkpattern.org website lists what are considered to be the most common techniques of manipulation. Some examples of these tricks, which are covered in our research, are known as *Roach Motel*, *Privacy Zuckering*, *Disguised Ads* and *Friend Spam*. *Roach Motel* is a graphical interface that makes it easy to subscribe, register, or sign-up for a service but more difficult to cancel this operation at a later juncture. *Privacy Zuckering* refers to Facebook's (and its CEO, Mark Zuckerberg) early strategies of presenting obscure "Terms and Conditions" and

"Privacy Policies" that tricks users into publicly sharing more of their personal information. *Disguised Ads* are advertisements disguised as other types of navigation content. *Friend Spam* consists of requesting email or social media permissions to present a desirable outcome for the user (e.g., connecting with friends) but then spamming the user's contacts.

Internet users frequently cite a lack of understanding to justify their privacy choices (Brandimarte, 2013, Williams et al., 2017). Some researchers argue that awareness about privacy choices and their negative consequences is the first—although not only—necessary step to mitigate data disclosure (Deuker, 2010; Pötzsch, 2009). Disclosing or releasing personal information is the conscious action of willingly sharing some information that is private or individually identifiable with a certain individual or group. Therefore, it is important to educate citizens about the existence of dark patterns aiming to circumvent their awareness, while informing them of the increasing importance of protecting their data privacy. Serious games are one way to achieve this and have been considered an effective strategy to train and educate users on varied topics (Alamri et al., 2013). More specifically, as Jost and Divitini argue (2021:16): *Competitive games with a scoring mechanism have advantages from an educator viewpoint as they are easily explained in teaching scenarios and quantifiable for comparative evaluation of learning progress*. This was the motivation for the development of a serious, competitive game aimed at informing individuals about such deceptive mechanisms used by many organizations. In order to understand this in more depth, we invited participants to play a game and measured their degrees of understanding of the dark patterns and risks. Subsequently, we evaluated if these variables were predictive of higher intention of engaging in privacy protection.

2. Method

2.1 Participants

The participants in this research were 56 high school students aged ranging from 16 to 18 years old; 32 female and 24 male students. These 56 are the students who played both the game and used at least 4 minutes on the questionnaire without providing the same response (for instance 3) for most of the questions. In a survey, if a respondent clicks on the same number, for example, 6 (=extremely likely) for all or almost all of the questions, the respondents will be deleted from the dataset being regarded as untrustworthy responses. This answering pattern indicates that the respondent either did not read the question or that no thought was given to their response.

2.2 Procedure

Participants were recruited in three upper secondary schools: one school in Copenhagen, Denmark, and two schools in Oslo, Norway. The research was conducted in the school classroom within a 50-min class. The participants were required to play The *Dark Patterns Game*, then answer a questionnaire.

First, each class teacher divided participating students into groups of 4 or 5, some groups including both genders and some with one gender only. Next, the students watched a short introduction and a 90-second video published on Vimeo about the game. Then, the students took part in a rehearsal session that lasted approximately 15 minutes. The game itself has a duration of 20-30 minutes per round. While playing the game, the students read or skimmed through the printed manual of game rules. For those requiring further information, the teacher and one representative from the developers answered questions about the rules and how to play. Finally, after the rehearsal, the students started to play the game. After finishing the game, the students calculated the score for each player, and based on the game score, the winner of the game was declared. When the students had finished playing, they were asked to fill out a questionnaire, which they could access on their own mobile phones.

2.3 The Game

The *Dark Pattern Game* was developed in collaboration by the company *Serious Games Interactive* and the Norwegian Computing Center, a non-profit private foundation. It was inspired by the master thesis, Serious Interactive Board Games: Increasing Awareness of Dark Patterns in Teenagers written by K. M. Nyvoll (Nyvoll, 2020). To the best of our knowledge, we are not aware of other dark pattern games aimed specifically at this age group and for this purpose. The game design was intended to be endogenous in form, where there is a close overlap between game mechanics and learning objectives to increase retention and transfer (Egenfeldt-Nielsen, 2019).

The *Dark Patterns Game* is a board game to be played in groups of three, four, or five people. Although the game is about apps, it is presented in a physical rather than digital format (that is, as a printed board game). The game contains a mobile-shaped board with nine app slots, five player-boards, dark pattern cards, fictitious apps, and cubes representing data types. The cards describe the name of the dark patterns, their mechanisms, and their consequences for users. Examples of cards and apps are presented in figures 2 and 3.

The first information players receive in the manual is*: "You just got a brand-new phone. You all want your type of apps on the phone (dating, SoMe, games, health, shopping) without giving away too much data about yourself*." Therefore, first, each player must choose a Player Board that defines one of the following roles: the Shopper, the Gamer, the Influencer, the Lover, and the Healthy. When playing, apps must be chosen according to the role. For example, the Shopper must install shopper apps on the mobile board, the Gamer must install gaming apps on the mobile board, and so on. Examples of cards and apps are presented in figures 2 and 3, presented in the next section.

The goal of the game is to have installed most of your assigned apps on the phone board without giving away too much personal data. Every time the player installs an app they must give away one or more data types. Besides, they must draw a Dark Pattern card that forces them to give away further data that they did not mean to. Consequently, the game requires players to deal with the decision of which apps to install, while being informed about the risks posed by the Dark Patterns, but in a playful manner. The player earns points by installing apps and loses points by granting data access permissions (the greater the number and type of data accessed by the apps, the greater the loss of points).

Figure 1 shows a *Plapp store* with 9 apps, with each player starting with two Dark Pattern cards as well as cubes with different colours signifying types of data. To start the game, 9 apps are placed face-up on each *App slot* on the *Plapp Store*, as shown in Figure 1. The other apps are placed face-down on the *App Pile slot*. Nine Dark Pattern cards are placed on the phone board. All apps have names. Examples of names are *Boomerbook, MeTube,* and *Poke Gogo* – see Figure 2. The names may be associated with apps available in the real world, but no actual names of apps are used.

The game progresses by a player taking and reading aloud the Dark Pattern card (Fig 3.) drawn from the phone slot - and then performing the required action, including placing cubes next to the app in question. The data cubes represent data-sharing; red is contact data, blue is media data, green is camera data and purple is location data. To win the game a player must install several apps while attempting to discard or avoid collecting as many data cubes as possible.

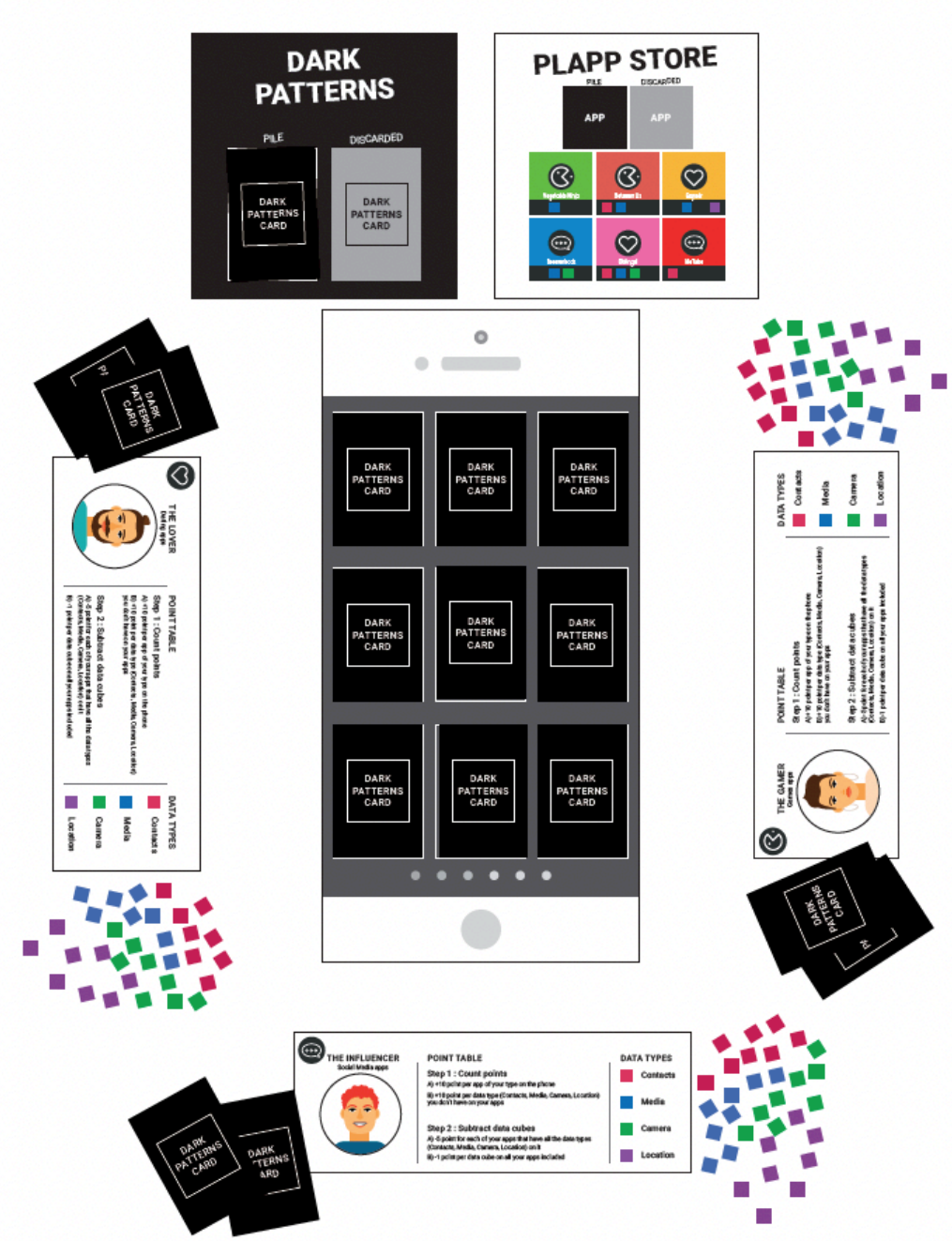

Figure 1: The set-up for the game-board with 3 players

Figure 2: The apps Boomerbook, MeTube and Poke Gogo

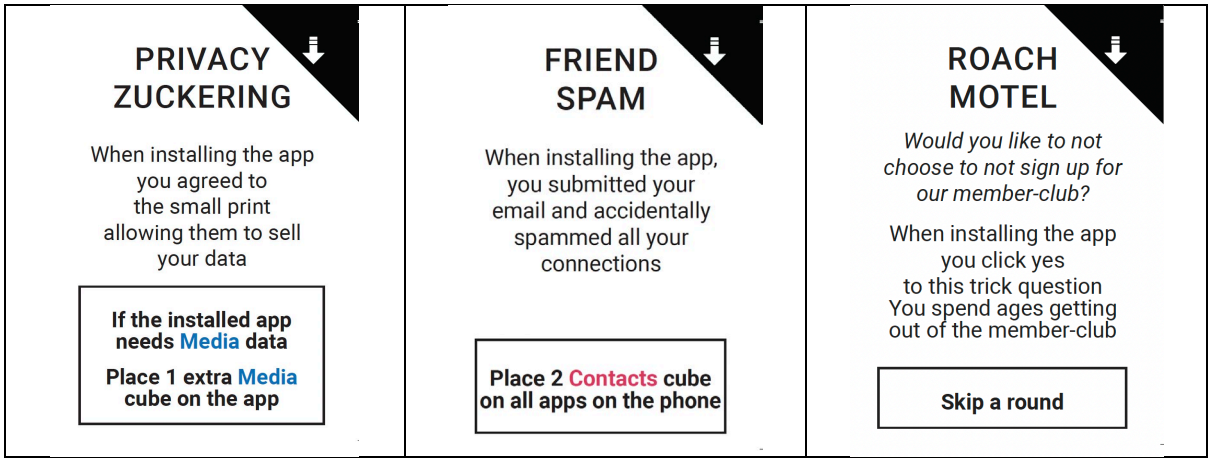

Figure 3: The Dark Pattern cards: Privacy Zuckering, Friend's Spam and Roach Motel

The rulebook for the game is the players' manual. This is available during gameplay and contains illustrations and information about how to calculate the score at the end of the game.

By reading the Dark Patterns cards and making choices about apps and cubes, the players learn about what can happen in the digital economy, along with the consequences of data-sharing. In Norway and Denmark, learning about the digital economy and developing digital judgment skills is part of the curriculum for students at upper secondary schools.

2.4 Questionnaire Measures

A battery of items measured the degree of self-reported knowledge about dark patterns, e-privacy risk perception in relation to dark patterns, and intention of performing privacy-protective behaviours. Risk perception was measured in two dimensions (probability and harm). Table 2 and 3 contain the questions (formulations) for each of the dark pattern types presented in the analysis in the results section.

2.5 Research question

There is not a finite list of dark pattern types. Some of the most common are listed by darkpattern.org. Not all, but several of the listed types are included in the Dark Pattern game.

This study was designed to understand how older teenagers respond to issues of personal data collection and (mis)use, through playing the *Dark Patterns game*, which involved them interacting with a smaller group of their peers. The questionnaire was designed to understand their experiences of playing and any knowledge gained. We have not identified scales or measurements for dark pattern types. The measurements in our work were developed by members of the research team. Consequently, we use the label "exploratory" for this research work. We formulated the following research questions targeted at students playing the game.

RQ1 To what extent did the game convey the meaning of the types of dark patterns presented in the game to the players?

RQ2 To what extent are the players of the games' risk perception of data-sharing, (the harmful consequences of data-sharing together with the probability of dark pattern incidents) associated with the intention to protect personal data?

RQ3. Is gender associated with the intention to protect personal data?

To answer these research questions, we analysed the data from 56 players with the Statistical method Partial Least Square – Structural Equation modelling (PLS-SEM).

3. Results

The questionnaire presented types of actual dark patterns. The next table presents percentages that reported that they understood the meaning or could explain the types used in the game.

Table 1: Questions about dark patterns

Dark patterns are activities to trick internet users into doing things they might not otherwise do. How much do you know about the following types of dark patterns?	Don't know what it means vs. I have a basic understanding, or I can explain the expression
Uninstall Shaming	61% - 39%
Roach Motel	86% - 14%
Disguised Ads	43% - **57%**
Friend Spam	54% - 46%
Privacy Zuckering	77% - 23%

Table 1 presents five types of dark patterns. There was only one instance where the majority of the respondents reported that they understood the type, for *Disguised Ads* 57% of respondents declaring that they understood or could explain its meaning.

For the Partial Least Square – Structural Equation modelling (PLS-SEM), as shown below, we created a variable named risk that is based on the answers to two questions. The questions with answers are presented in table 2 and 3. We used Likert scales for the answers, ranging from never (1) to always (5), from no harm (1) to extreme harm (6), and from not likely (1) to extremely likely (7). Questions with the answers 1, 2 and 3 are coded as low, 4 is coded as medium and 5, 6, and 7 are coded as high.

Table 2: How data are used by companies and perceived harm - related to 5 dark pattern types

To what extent do the following agreements/technologies feel harmful to you?	Low-medium-high
When installing an app, the install app button appeared as "download now". You clicked on the button and rather than downloading the app you were redirected to a website advertising another product. *Disguised Ads*	19% - 27% - **54%**
When installing an app, you accepted the invitation to join a one-month free member club (without knowing the conditions). *Roach Motel*	25% - 18% - **57%**
When uninstalling an app, you received a message shaming your decision. For example, "Do you really want to uninstall this game which was practically the only fun you had? Your life will be sad and gray without it!" *Uninstall Shaming*	56% - 14% - 30%
When installing an app, you gave the access to your email account on the premise that it will give you "a strong network". *Friend Spam*	31% – 23% - 46%
When installing an app, you agreed to the small print. *Privacy Zuckering*	36% – 25% - 39%

Table 2 shows that *Roach Motel* and *Disguised Ads* are perceived as the two most harmful exhibiting 57% and 54% high probability. In the PLS-SEM analysis, the risk variable is created by multiplying the score on each of these 5 with the similar 5 in table 3. For instance, 6 (=extreme harm) on *Disguised Ads* is multiplied with 6 (extremely likely) on *Disguised Ads* on how likely this incident is. Following this a scale was created; score 1 to 5 =1, 6 to 11 = 2, 12 to 17 =3, 18 to 23 =4, 24 to 29 =5, and 30 to 36 = 6. In the example with *Disguised Ads*, 36 equates to 6 on the Risk scale. In the two PLS-models we use the name PerceivedRisk_due_to_DarkPattern_activities.

In the next table, table 3, the questions about probability of experiencing the 5 types of dark pattern are presented. The scale is from *not at all* likely to *extremely likely*. The answers are summarized and presented in the right-hand column.

Table 3 Expectations - what do you think could happen? Five dark pattern types

HHow likely do you think it is that you will experience the following?	
	Low-medium-high
The install app button appears as "download now". You click on the button and, rather than downloading the app, you are redirected to a website advertising another product and starts seeing ads of that product everywhere on the internet. *Disguised Ads*	46% - 21% - 33%
You accept the invitation to join a one-month free member club and, then, you spend ages trying to cancel your membership. *Roach Motel*	50% - 18% - 32%
You give the app access to your email account on the premise that it will give you "a strong network" and the app spams all your connections asking them to join you in that app. *Friendship Spam*	46% - 18% - 36%
When uninstalling an app, you receive a message shaming your decision. For example, "Do you really want to uninstall this game which was practically the only gun you had." Your life will be sad and gray without it!" *Uninstall Shaming*	50% - 27% - 23%
When installing an app, you agree to the small print (without reading it) *Privacy Zuckering*	18% - 20% - **62%**

Table 3 shows that the respondents did not expect dark patterns often, expect for privacy zuckering with 62% high probability.

Table 4: Behavioural intentions – taking proactive steps

How often do you intend to perform the following actions in the next 30 days?	
	Never or rarely vs. sometimes or always
Putting a sticker on your camera making it impossible for apps to access your camera.	70% - 30%
Deleting and reinstalling an app to get rid of accumulated data the app had access to.	75% - 25%
Replacing apps for similar ones that require access to fewer data to function.	86% - 14%
Revising your app's permission setting so that the app is unable to access some data.	56% - **44%**

As can be seen, the majority of the respondents are not planning to take proactive steps to protect their data. Revising apps' permissions is the response option with the highest percentage, 44% - see table 4.

3.1 Partial Least Square – Structural Equation Modelling

PLS-SEM has become one of the standard tools for analysing inter-relationships between observed and latent variables in social science research (Sarstedt et al. 2019). This structural equation modelling technique can simultaneously estimate measurement components and structural components, that is, the relationships between constructs. PLS path-modeling enables the maximization of explained variance of all dependent variables and thus supports prediction-oriented goals (Henseler, 2009). With PLS-SEM it is not a prerequisite that research models are based on comprehensive theories (Barclay et al., 1995; Chin, Marcolin and Newsted, 2003), and therefore one of the reasons why it is common to use PLS-SEM in exploratory research and sometimes in the early stages of a research project.

The minimum sample size required by PLS-SEM is seven to ten times the larger number of paths leading to an endogenous construct when, as is the case in this study, all constructs except for gender are reflective (Chin et al. 2003). Convergent validity is suggested if factor loadings are 0.60 or higher (Bagozzi and Yi, 1988) and each item loads significantly on its latent construct (Gefen and Straub, 2005). Discriminant validity is suggested if all measurement items load more strongly on their respective construct than on other constructs. The square root of average variance extracted (AVE) of each construct should be higher than the inter-construct correlations – the correlations between that construct and any other constructs (Fornell and Larcker, 1981). An AVE above the recommended threshold of 0.5 indicates a satisfactory level of convergent validity. For further information about PLS as a statistical method, we refer to Chin (1998).

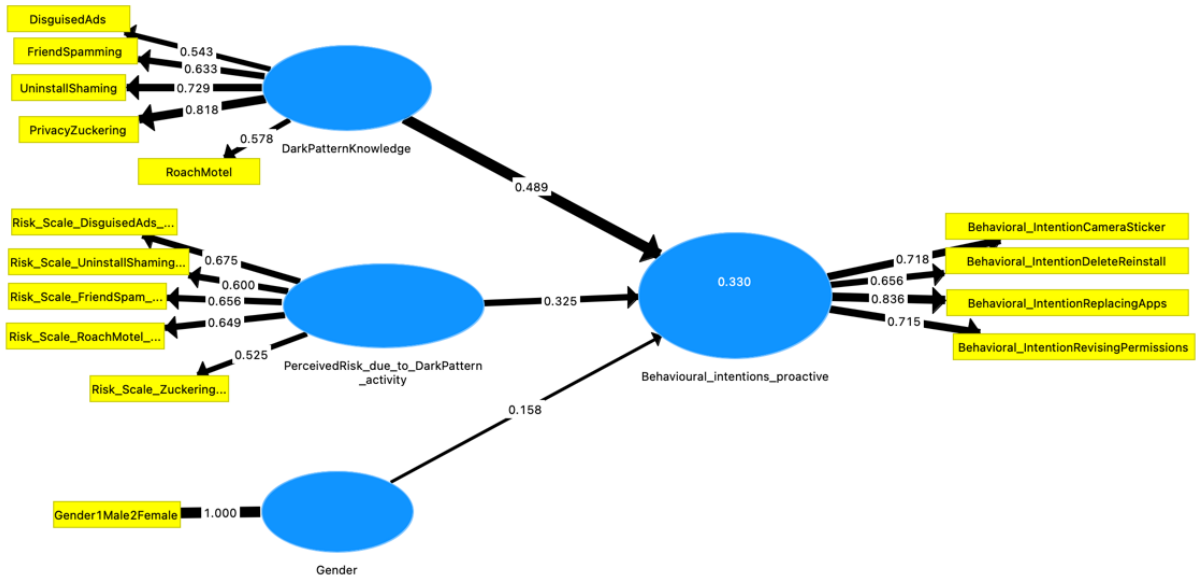

Figure 4: PLS model 1 - Dark pattern knowledge, perceived risk and gender as predictors

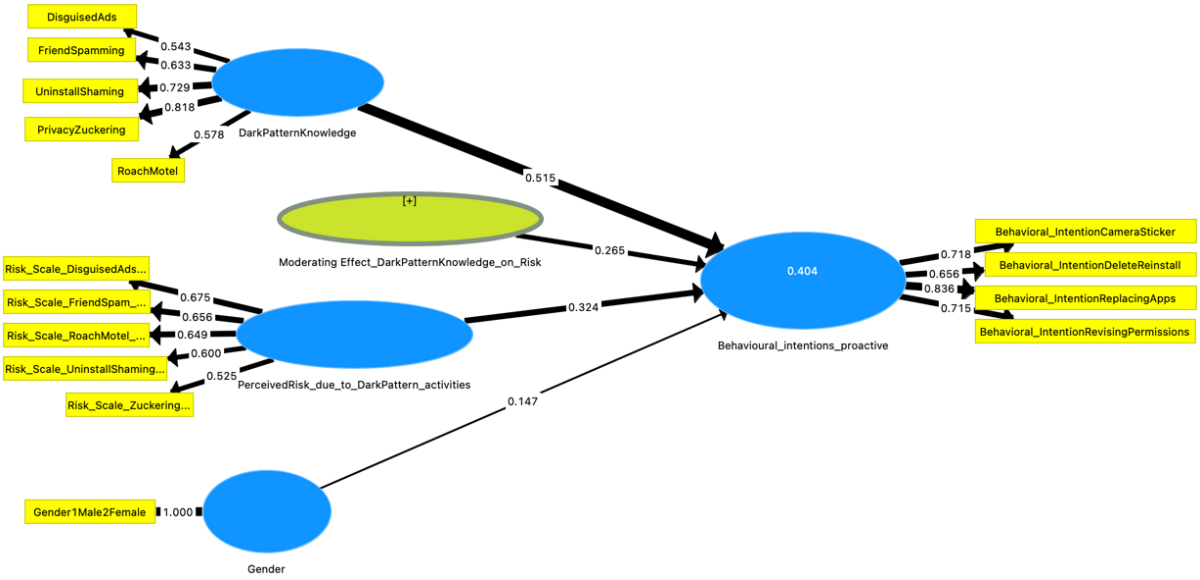

Figure 5: PLS model 2 - Dark pattern knowledge, perceived risk and gender as predictors with dark pattern knowledge as moderator.

In the figures, the thickness of the lines (also known as paths in the PLS-terminology) indicates the strengths of the association. Both dark pattern knowledge and perceived risk are significant predictors, whereas gender is not.

In the first PLS – model 1 the variance explained is 0.33 while in the PLS-model 2 it has increased to 0.4. According to Chin (1998) both register a moderate level. There is no simple answer to what is (or interpreted as) a high, moderate, and low variance explained, but a moderate level can be seen as having reasonably good explanatory power. However, also the quality criterions have must also be discussed before a conclusion is made.

Table 5. The construct reliability and validity, and discriminant validity of the PLS path model

	Construct Reliability and Validity			**Discriminant Validity**			
	Cronbach's Alpha	**Composite Reliability**	**Average Variance Extracted (AVE)**	**Behavioural Intentions**	**DP knowledge**	**Gender**	**Perceived Risk**
Beh.Intentions	0.712	0.823	0.539	**0.734**			
DP knowledge	0.711	0.797	0.446	0.438	**0.668**		
Gender	1.00	1.00	1.00	0.092	-0.209	**1.00**	

	Construct Reliability and Validity			Discriminant Validity			
	Cronbach's Alpha	**Composite Reliability**	**Average Variance Extracted (AVE)**	**Behavioural Intentions**	**DP knowledge**	**Gender**	**Perceived Risk**
Perceived Risk	0.606	0.595	0.389	0.314	-0.057	0.11	**0.624**

According to Table 5 not all quality criterions for a sound PLS-models are met (Chin, 1998). Figure A shows that the item *Roach Motel* has loading of 0.578. This is below the threshold of 0.6 for items in exploratory studies. This is the reason why the average variance extracted, 0.446, is below the threshold of 0.5. If this item had been deleted, the quality criteria would have been met. Table 1 shows a low number (14%) on the question about explaining the expression roach motel. There are only three *Roach Motel* cards in the game, and not four or five as for the other dark pattern cards. The consequence is that in some games played by the students in this study, it is possible that none of the players got the *Roach Motel* card.

There is also an issue with the perceived risk factor. The (privacy) Zuckering item has an item-loading below 0.6, and the other items have loadings between 0.6 and 0.7. For a reliable measurement, the loadings should be at least 0.7. This is the reason why the composite reliability, a measurement for internal consistency, is below 0.6. The item named Zuckering could have been removed, but we decided to include the same types of items for the dark pattern knowledge and the perceived risk related to dark pattern activities.

4. Conclusion

Bellotti et al. (2013) write, "*Serious games are designed to have an impact on the target audience, which is beyond the pure entertainment aspect*." According to Zhonggen (2019), serious games are reported effective in education, but some studies arrive at negative conclusions. We used survey questions to measure the impact, if any, on the players of the Dark Patterns game. We conclude from the responses that the game had only a partial impact on the players' understanding and knowledge about dark patterns. The first research question (RQ1) was, *To what extent did the game convey the meaning of the types of dark patterns presented in the game to the players?* the players reported that they understand or can explain what the term means for only one of the dark pattern types - see table 1. One the other hand, knowledge about dark patterns matters. The PLS-SEM analysis shows that knowledge has a significant contribution in our model. The students with high dark pattern knowledge also report higher intention to take steps to protect their data. Of the three variables in the model, it is the most important and plays a role as moderator. We still conclude that RQ1 was not supported because most of the players stated that they could not explain the meaning of the dark pattern types.

The conclusion for the second research question is only based on the result of the PLS-SEM analysis. The analysis is exploratory in nature; we did not use constructs developed and validated by other researchers, but we developed questions specifically targeted to the types of dark patterns in the game. The second research question (RQ2) was, *To what extent are the players of the games' risk perception of data-sharing, (the harmful consequences of data-sharing together with the probability of dark pattern incidents) associated with the intention to protect personal data?* The PLS-SEM analysis shows a moderate association between the independent and dependent variables. In our model, dark pattern knowledge is the most important predictor followed by perceived risk. We conclude that RQ2 was supported.

The third research question, RQ3, was, *Is gender associated with the intention to protect personal data?* The PLS-SEM analysis showed that gender was not a significant predictor. Based on this result we conclude that RQ3 was not supported.

In the next phase of the research project on the dark pattern game, we will focus on students that have played the game several times. It is likely that a player that would like to win the game would need to practice, to play more than once. Then the player can make choices and think about which cards to play, and when. We think that a better approach to understanding the question of learning would be to use the score, the result of the game, together with the answers to survey questions, and after a player has played the game at least twice.

Acknowledgements

This research was supported by Research Council Norway under the grant 270969, the research programme IKTpluss.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science,* 347(6221): 509-514.

Alamri, A., Hassan, M. M., Hossain, M. A., Al-Qurishi, M., Aldukhayyil, Y., & Hossain, M. S. (2013). Evaluating the impact of a cloud-based serious game on obese people. *Computers in Human Behavior,* Vol 30, pp. 468–475.

Bagozzi, R. P. & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16(1): 74-94.

Barclay, D. C., Higgins, C. & Thompson, R. (1995). The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies* 2(2): 285-308.

Bellotti, F., Kapralos, B., Lee, K., Moreno-Ger, P., & Berta, R. (2013). Assessment in and of serious games: an overview. *Advances in Human-Computer Interaction*, vol. 2013, 1, art.no. 136864.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy Engines and Data Retention: Implications for Privacy and the Control Paradox." *Social Psychological and Personality Science,* 4 (3): 340.

Brignull, H., Miquel, M., Rosenberg, J. & J. Offer (2015). Dark Patterns - User Interfaces Designed to Trick People. http://darkpatterns.org/

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (ed.), Modern methods for business research. Mahwah NJ: Lawrence Erlbaum Associates, pp. 295-358.

Chin, W. W., Marcolin, B. L. & Newsted, P. R. (2003). A partial least squares latent variables modeling approach for measuring interaction effects: Results from a Monte Carlo Simulation study and an electronic-mail emotion/adoption study. *Information Systems Research* 14(2): 189-217.

ciation Conference, Boston, MA, May 28. Payments Cards Center Discussion Paper 05-10.

Deuker, A. (2010). Addressing the privacy paradox by expanded privacy awareness – The example of context-aware services. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G. (eds) Privacy and Identity Management for Life. Privacy and Identity 2009. *IFIP Advances in Information and Communication Technology*, Vol 320.

Egenfeldt-Nielsen, S., Smith, J. & Tosca S. (2019). Understanding Video Games. Chapter 8. Routledge.

Gefen, D. & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the AIS* 16(5): 91-109.

Henseler, J., Ringle, C.M., & Sinkovics, R.R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing* 20: 277-320.

Jost, P., & Divitini, M. (2021). Designing Analytic Serious Games: An Expert Affordance View on Privacy Decision-Making. In: Fletcher B., Ma M., Göbel S., Baalsrud Hauge J., Marsh T. (eds) Serious Games. JCSG 2021. *Lecture Notes in Computer Science*, vol 12945. Springer, Cham. https://doi.org/10.1007/978-3-030-88272-3_1

Nyvoll, K. M. (2020). Serious Interactive Board Games: Increasing Awareness of Dark Patterns in Teenagers, Master's thesis, Department of Computer Science at the Norwegian University of Science and Technology (NTNU)

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In: Matyáš, V., Fischer-Hübner,

S., Cvrček, D., Švenda, P. (eds) The Future of Identity in the Information Society. Privacy and Identity 2008. *IFIP Advances in Information and Communication Technology*, Vol 298.

Sarstedt, M., Ringle, C.M., Cheah, J.-H., Ting, H., Moisescu, O.I. & Radomir, L. (2019). Structural model robustness checks in PLS-SEM, *Tourism Economics*, 1-24.

Williams, M., Nurse, J. R. C., & Creesen S. (2017). Privacy is the boring bit: User perceptions and behaviour in the Internet-of-Things. *15th Annual Conference on Privacy, Security and Trust (PST)*, pp. 181–190.

Zhonggen, Y. (2019). A Meta-analysis of use of serious games in education over a decade. *International Journal of Computer Games Technology*, 5 (1) 2019, pp. 1-8.