Technology-based Privacy Protection Tools

A study about the factors influencing the decision of Internet users' to adopt and use technology-based privacy protection tools

Master Thesis | Ajosha Thenu

UNIVERSITY OF TWENTE.

Detailed Information

Institute

University of Twente
Drienerlolaan 5
7522 NB Enschede

Faculty and Program

Faculty of Behavioral Sciences
MSc Communication Studies
Marketing Communication and Consumer Behavior

Graduation Committee

Dr. A. D. Beldad
Dr. S. A. de Vries

Author

Ajosha Thenu
S1492764

Date

28.07.2015

Abstract

This research aims at gaining insight into the intention to adopt technology-based privacy protection tools. It does so by testing the core of the Unified Theory of Acceptance and Use of Technology model, and adding variables from the Protection Motivation Theory that are essential for understanding user acceptance in the context of TBPPT. Using an online questionnaire, 580 responses were collected of which 326 were used for analysis. The respondents were divided in two groups: non-users, and users of TBPPT and analyzed separately using hierarchical regression analysis. The findings of this research imply that social influence, facilitating conditions, and intrinsic rewards are significant predictors of the intention to adopt TBPPT, and performance expectancy, facilitating conditions, perceived severity, and intrinsic rewards to be significant prediction of TBPPT usage. Although not all the hypothesized variables were found significant predictors, this research has laid the foundation for a model that can explain user acceptance in the context of TBPPT, the Online Privacy Protection Model.

Keywords:
Unified Theory of Acceptance and Use of Technology
Protection Motivation Theory
Online Privacy Protection Model
Technology-based Privacy Protection Tools

Acknowledgements

This thesis is the final part of my Master Communication Studies, and will conclude the degree I have earned at the Universiteit Twente. I enjoyed specializing myself in Marketing Communication and Consumer Behavior and am thankful for the opportunity to combine the knowledge obtained from the Master's courses with my area of interest: Online Privacy Protection.

Throughout the past two years many people have continuously supported me in many ways and this is the moment to acknowledge my gratitude. First of all, I would like to thank my family and friends for their encouragement and help. I would specifically like to thank my better half Carolyn Krogoll, who supported me throughout the process of writing my thesis. Secondly, I would like to thank the staff of the study program for sharing their wisdom, expertise and professional insights.

And most importantly, I would like to express my gratitude to my supervisors Dr. Ardion Beldad and Dr. Sjoerd de Vries - this thesis would not have been possible without you. I highly appreciate your academic professionalism, critical feedback, as well as the patience and inspiration you brought in working with me – Thank you!

Enschede, July 2015

Ajosha Thenu

Table of Contents

List of Figures

List of Tables

1. Introduction

Ever since the creation of the Internet in the 1990's it has grown exponentially. We have come to a point where almost any product, service, or information can be found or purchased on the Internet. Although the Internet might seem to provide these services for free, it does not sustain itself. When services or information are seemingly offered free of cost, it is almost a certainty that the Internet user is paying with some kind of commodity. Currently the most popular commodity used for paying for free content is personal information.

More than often Internet users offer up their personal information willingly, and without considering the possible consequences. For example, many websites require the Internet user to sign up before the Internet user is allowed to make use of any content or services. This is often done for obvious reasons, such as providing personal information to make an account, to sign up for a news-letter, to participate in a contest, or to have a product send to your home. In such instances the Internet user can make trade-offs on what information they would like to share with the website, and what information they would not like to share. Often the website will offer terms of agreement with which the Internet user has to comply before gaining access to the products/ services to be bought.

Though Internet users can make their own decisions regarding personal information trade-offs when they sign up for online services, they have no control over what information gets gathered while they browse the Internet in general. While browsing the Internet, both personally identifiable information, and non-personal identifiable information can be collected and stored without the knowledge of the Internet user. This practice is called "third-party tracking".

Many Internet users are not aware of the collection of personal information by third-parties (Smit, van Noort, & Voorveld, 2013). Due to the growing amount and increasing variety of personal information tracked by third party trackers, programmes such as technology-based privacy protection tools (TBPPT) have enjoyed increased popularity. These TBPPT are either software or browser add-ons which prevent third-parties from collecting personal information from the Internet user. However, if Internet users do not use or even know about TBPPT, what can be done to positively influence their consideration to obtain, install, and use TBPPT? The case of TBPPT adoption could be tested against several existing models, such as the Technology Acceptance Model (Davis, 1989), the Theory of Planned Behavior (Ajzen, 1991), or the Unified Theory of Acceptance and Use of Technology (Venkatesh, Morris, Davis, and Davis, 2003). However, there exists no concrete theory that addresses the core problem in the adoption of TBPPT, which is the assessment of a threat. When Internet users learn about the practice of third-party tracking, more than benefits, usefulness, social norms, or effort expectancy is assessed, they will initially be driven by the fear of losing personal information.

This begs us to ask the question: "What factors influence the decision of Internet users' to adopt and use technology-based privacy protection tools?". This study will attempt to answer this research question by combining the Unified Theory of Acceptance and Technology use with variables from a model from the healthcare field, the Protection Motivation Theory (Rogers, 1975).The Protection Motivation theory does not only take into account the consideration of benefits, but the threats as well. Furthermore, this study will address the perspective of two different types of respondents, those who do not use TBPPT, and those who do use TBPPT.

This research will be tested against a sample of the population from the Netherlands. With 95.7% Internet users on it's entire population (IWS,2015) and above average Internet skills compared to other countries in Europe (CBS, 2014), the Netherlands represents a country with "experienced" Internet users.

The adjacent section will the Theoretical Framework, in which potential variables that predict the intention to adopt and system usage will attempted to be identified, as well as the formulation of the corresponding hypotheses. Section four will focus on the methods used in executing this research, elaborating on the research design, procedure, participants, measurements, and the reliability of the measurement instrument. The fifth section will present the results of this research. Section sic, the final section, will discuss the results, give advice for practical implications, explain the theoretical relevance, and conclude on this research.

2. Theoretical framework

To answer the research question of "What factors that influence the decision of Internet users' to use technology-based privacy protection tools?" the theoretical landscape surrounding the research question will first be explored. When trying to understand any process relating to the adoption of technology it is almost imperative to consider the Technology Acceptance Model (TAM). The evolution of the TAM has been explaining user acceptance since 1989 when Davis published the first version. The TAM has gone through two improvements since then TAM2, by Venkatesh and Davis (2000), and TAM3 (2008), by Venkatesh and Bala. Taking the core idea of the TAM, and combining it with other established variables from existing literature, Ventakesh, Morris, Davis, & Davis reworked the existing dominant user acceptance models into a model called the Unified Theory of Acceptance and Use of Technology (UTAUT). The UTAUT consists of four core variables: effort expectancy (EE), performance expectancy (PE), social influence (SI), and facilitating conditions (FC) and "assesses the likelihood of success for new technology introductions" in an organizational context (Venkatesh et al., 2003, p 425-426).

The UTAUT has a successor in the form of UTAUT2 (Venkatesh, Thong, & Xu, 2012), in which it has had three variables added; hedonic motivation, price value, and habit and lies it focuses on a consumer user acceptance context. However, the three added variables of the UTAUT2 fail to add sufficient value to the context of this research to justify using them, and therefore this research will incorporate the more compact and generally applicable UTAUT model.

However, the process of engaging in the usage of TBPPT does not limit itself to the functional and facilitating aspects that the UTAUT addresses. The usage of TBPPT comes with both benefits and costs. An Internet user might be more protected against third-party tracking, but could potentially experience a decrease in Internet browsing convenience. The Internet user therefore has to weigh the perceived benefits of using TBPPT against not only the perceived threat, but against the costs as well. An established model that assesses both the benefits, threat, and costs of adoption in relation to protecting oneself is the Protection Motivation Theory (PMT) by (Rogers, 1975). In its original state, the PMT addressed only "the magnitude of noxiousness of a depicted event, the conditional probability that the event will occur if no adaptive activity is performed, and the effectiveness of a coping response that might avert the noxious event" (Rogers & Mewborn, 1976, p. 55). As the model developed, three more variables were added to the existing variables of perceived vulnerability (VUL), perceived severity (SEV), and response-efficacy (RE), namely; intrinsic rewards (IRW), extrinsic rewards (ERW), self-efficacy (SE), and response costs (RC) (Floyd, Prentice-Dunn, & Rogers, 2000).

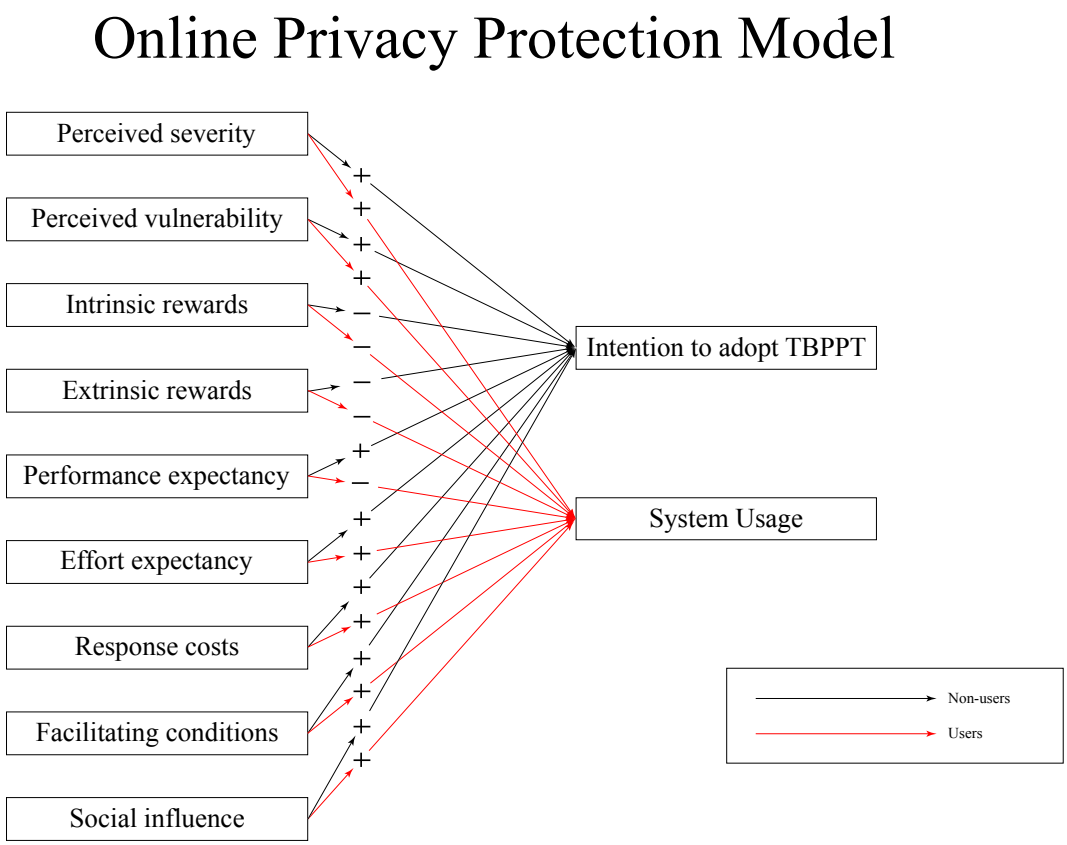
PMT divides these seven variables into two categories: threat appraisal and coping appraisal. Threat appraisal assesses the maladaptive behaviour (Floyd et al., 2000), weighing SEV and VUL against the potential IRW and ERW. The coping appraisal is an evaluation of both the perceived ability to perform the recommended behaviour and its ability to avert the perceived threat, and is comprised of the RE and SE, which is weighted against the perceived RC (Floyd et al., 2000). The resulting attitudes towards the appraised threat and recommended coping behaviour are then considered prior to deciding whether to engage in a maladaptive response, or adoption of the recommended behaviour (Rogers & Mewborn, 1976).

The main model that will be used in this research will be the one of UTAUT, which will be complemented with variables form the PMT. However, some variables, such as self-efficacy (SE) and response-efficacy (RE), will be excluded from the model, as they would overlap

some of the UTAUT variables. The EE variable form the UTAUT for example, entails whether the Internet user expects that using TBPPT will be free of effort (Venkatesh et al., 2003). The counterpart EE from the PMT could be considered to be SE, and implies whether an Internet user believes that they can perform the recommended behaviour based on their own efficacy and mastery (Maddux & Rogers, 1989). RE, on the other hand, entails whether the Internet user believes the recommended behaviour effectively averts the potential threat (Woon, Tan, & Low, 2005, p. 370). This concept is covered by the UTAUT's PE, which is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance (p. 320)."

Having identified all variables for the research model to be tested, they can be put into a Online Privacy Protection Model (see Fig. 1). This chapter will now go further into detail of the different variables, and their accompanying hypotheses.

Figure 1:



2.1 Perceived severity (SEV)

Rogers and Mewborn (1976) define perceived severity (SEV) as "the magnitude of noxiousness of a depicted event" (p. 55). Applying PS to the context of this research, it entails that the Internet user needs to perceive a sufficiently high enough level of severity of the threat before they would consider adopting TBPPT. Asides from it's use health-related studies, the concept of PS has been found to be a significant positive predictor of user acceptance in a variety of technology-related cases, such as protective technologies (Chenoweth, Minch, & Gattiker, 2009) and home wireless security (Woon, Tan, & Low, 2005). However, more often than not SEV appears to be found a non-significant predictor of the intention to adopt, specifically in realtion to virus protection (Lee, Larose, & Rifon,

2008), password change (Zhang & McDowell, 2009), and mobile health services (Sun, Wang, Guo, & Peng, 2013). Lee, Larose, and Rifon (2008) argued that the non-significant effect of SV could be attributed to VUL, as a person might assess a specific threat to be severe, but if they estimate a low probability of occurrence to them specifically, they might not feel the need to adopt TBPPT. In the specific case of TBPPT, it makes sense that an Internet user needs to perceive the threat of third-party tracking as severe prior being able to decide whether or not to engage in using TBPPT. For this it is hypothesized that:

H1a: Perceived severity positively influences the behavioural intention of non-users to adopt and use technology-based privacy protection tools.
H1b: Perceived severity positively influences the current users' system usage of technology-based privacy protection tools.

2.2 Perceived vulnerability (VUL)

Together with SEV, perceived severity (VUL) makes up the threat appraisal. Maddux and Rogers (1989) define VUL as the "probability of the occurrence of the event" (p. 470). Putting this definition into perspective for this research, VUL is defined as the probability the Internet user estimates of becoming a victim to loss of privacy due to third-party tracking. VUL has proven to be a significant predictor of user acceptance in a variety of technology-related studies, such as virus protection (Lee, Larose, & Rifon, 2008), and protective technologies (Chenoweth, Minch, & Gattiker, 2009). VUL has been found to be an insignificant predictor of the intention to adopt as well in studies regarding home wireless security (Woon, Tan, & Low, 2005) and virus protection (Lee Larose, & Rifon, 2008). If Internet users believe that the proposed threat of loss of personal information through third-party tracking is probable to occur to them specifically, they will be more likely to engage in the use of TBPPT. Therefore it is hypothesized that:

H2a: Perceived vulnerability positively influences the behavioural Intention of non-users to adopt and use technology-based privacy protection tools.
H2b: Perceived vulnerability positively influences the current users' system usage of technology-based privacy protection tools.

2.3 Rewards (IRW & ERW)

The perceived threat is then weighted against the perceived rewards associated with the maladaptive behaviour. This is done on two levels; by intrinsic rewards, which cover the perceived direct and personal gain from engaging in the risk behaviour, and extrinsic rewards, which assess "the perceived positive effects in relation to ethical responsibility from engaging in a maladaptive response" (McDonell et al., 2013).

In relation to the context of this study intrinsic rewards refer to any positive gain from not installing/ using TBPPT. One of the few advantages from not installing/ using TBPPT is online behavioural advertising. In a study examining user concerns for online tracking and advertising by Agarwal et al. (2013), found that although concerns for third-party tracking and online behavioural advertising exists, participants were more concerned about being presented embarrassing advertisements in front of peers.

Extrinsic rewards could be supporting the website you like, or the Internet in general, but essentially comes down to playing your part in the Internet ecosystem. With an increasing number of Internet users blocking trackers and OBA, websites have resorted to custom messages informing the Internet user that they are blocking the income of the website by blocking their advertisements, pleading for the Internet user to allow the advertisements so

that the website can sustain itself. These websites are appealing to the ethical responsibility of the Internet user to take part in the Internet ecosystem, and that the Internet user does their share of give and take. For this it is hypothesized that:

H3a: Intrinsic rewards negatively influence the behavioural intention of non-users to adopt and use technology-based privacy protection tools.
H3b: Intrinsic rewards negatively influence the current users' system usage of technology-based privacy protection tools.
H4a: Extrinsic rewards negatively influence the behavioural Intention of non-users to adopt and use technology-based privacy protection tools.
H4b: Extrinsic rewards negatively influence the current users' system usage of technology-based privacy protection tools.

2.4 Performance expectancy (PE)

Performance expectancy (PE) is defined by Venkatesh et al. (2003) as "the degree to which a person believes that using a particular system would enhance his or her job performance (p. 320)." Venkatesh et al. used five constructs form existing literature to establish performance expectancy, namely; perceived usefulness, extrinsic motivation, job-fit, relative advantage, and outcome expectancies. For the purpose of this research performance expectancy will be redefined to: "Performance expectancy is the degree to which an individual believes that using TBPPT will help him or her to attain gains in online privacy protection." In previous research both performance expectancy (Luo, Li, Zhang, & Shim, 2010; Venkatesh et al., 2003) and its equivalent response efficacy (Sun, Wang, Guo, & Peng, 2013) from the PMT have been found to be the strongest predictor of the intention to adopt in both technological and health-related research. More specifically, studies into mobile banking (Luo, Li, Zhang, & Shim, 2010; Zhou, Lu, & Wang, 2010; Martins, Oliveira, & Popovic, 2014), location-based services (Zhou, 2012; Yun, Han, & Lee, 2013) and healthcare information systems (Hsu & Lee, 2012) have all identified PE as a significant predictor of the intention to adopt. It is expected that an assessment of the PE will be made prior to adopting the TBPPT by the Internet user. Therefore, it is hypothesized that:

H5a: Performance expectancy positively influences the behavioural intention of non-users to adopt and use technology-based privacy protection tools.
H5b: Performance expectancy positively influences the current users' system usage of technology-based privacy protection tools.

2.5 Effort expectancy (EE)

Venkatesh et al. (2003) defined effort expectancy as "the degree to which a person believes that using a particular system would be free of effort (p. 320)." As with performance expectancy, effort expectancy was conceptualized based on three constructs derived from related existing models; perceived ease of use, complexity and ease of use (Venkatesh et al., 2003). Even though considered as one of the core constructs of the UTAUT, the applicability of effort expectancy appears to be dependent on the context as existing literature presents diversity in findings. For instance, significant findings have been found in relation to general (Im, Hong, & kang, 2011) and innovative technology user acceptance (Casey & Wilson-Evered), and Internet banking (Martins, Oliveira, & Popovic, 2014), whereas non-significant results have been found in healthcare information systems (Hsu & Lee, 2012). For this it is hypothesized that:

H6a: Effort expectancy positively influences the behavioural intention of non-users to adopt and use technology-based privacy protection tools.

H6b: Effort expectancy positively influences the current users' system usage of technology-based privacy protection tools.

2.6 Response costs (RC)

According to the PMT, the Internet user appraises the perceived effectiveness and required effort of the recommended behaviour, which are then weighted against the perceived response costs. Literature defines response costs as "an estimate of the costs associated with a particular course of action (Neuwrith, Dunwoody, & Griffin, 2000, p. 723)."

Several other technology acceptance-related studies have applied response costs significantly to behavioural intention in the context of home wireless security and using protective passwords amongst others (Woon, Tan, & Low, 2005; Chenoweth, Minch, and Gattiker, 2009; Zhang & McDowell, 2009). Within this research, response costs are considered any time, effort investments, or reduction in convenience caused by installing/ using TBPPT. Depending on the type of TBPPT using it can substantially impact the fluency of using the Internet. Some TBPPT block any media players/ advertisements whilst Internet users might want to see either one of them. Though often there exists an option to turn the TBPPT off or even whitelist a site, it can be considered an inconvenience while browsing the Internet. Furthermore, even if only browser settings are used to remove cookies or clear history, it can impact convenience. Cookies are the files that remember your username, password and much more preferences it might have gathered on the Internet user's browsing behaviour. For this it is hypothesized that:

H7a: Response costs negatively influence the behavioural intention of non-users to adopt and use technology-based privacy protection tools.
H7b: Response costs negatively influence the current users' system usage of technology-based privacy protection tools.

2.7 Social influence (SI)

Social influence is defined as "the degree to which an individual perceives that important others believe he or she should use the new system" (Venkatesh et al, 2003, p. 451). Social influence originates from three other constructs from recognized academic literature; subjective norm, social factors, and image (Venkatesh et al., 2003). In the context of this research social influence will most likely come from friends, family and/or co-workers. It is a fair assumption that non-users were made aware either by someone from their social environment, or by self-education. Regardless of the source, the process of informing on third-party tracking will most likely have included some kind of mention of TBPPT as well. SI is a core construct of the UTAUT and has been proven a significant predictor to user acceptance in studies relating to mobile banking (Zhou, Lu, & Wang, 2010; Martins, Oliveira, & Popovic, 2014), general (Im Hong, & Kang, 2011) and innovative technology adoption (Casey & Wilson-Evered, 2012), and healthcare information systems (Hsu & Lee, 2012). IHowver, a non-significant effect form SI on intention was found in a study into location-based service applications (Yun, Han, & Lee, 2013). Based on the existing literature it is expected that the social environment would play a significant role in the decision to adopt TBPPT for both non-users and users. For this reason it is hypothesized that:

H8a: Social influence positively influences the behavioural intention of non-users to adopt and use technology-based privacy protection tools.
H8b: Social influence positively influences the current users' system usage of technology-based privacy protection tools.

2.8 Facilitating conditions (FC)

Facilitating conditions are defined as "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system (Venkatesh et al, 2003, p. 453)." Facilitating conditions has been conceptualized with the intention to capture three existing variables; perceived behavioural control, facilitating conditions, and compatibility (Venkatesh et al., 2003). As this research does not take place within an organization, FC will redefined to better fit the context of this research. For this research FC will be defined as the degree to which an individual believes that and support exists to facilitate the learning and using of TBPPT. Although FC is a core construct of the UTAUT, it is most often tested against system usage over intention to adopt. FC has been found a significant predictor for the intention to adopt in a healthcare information system context (Hsu & Lee, 2012), and for system usage in the contexts of mobile banking (Zhou, Lu, & Wang, 2010), technology adoption (Im, Hong, & Kang, 2011) and location-based services (Zhou, 2012). It is expected that both users and non-users will find appreciate and require the presence of FC when deciding to adopt TBPPT. Therefore, it is hypothesized that:

H9a: Facilitating conditions positively influence the behavioural intention of non-users to adopt and use technology-based privacy protection tools.

H9b: Facilitating conditions positively influence the system usage of technology-based privacy protection tools.

3. Methods

3.1 Research design

This research uses a correlational design as it attempts to explore the direction and relationships between predictor, and outcome variables. The data will be collected by means of an online questionnaire, as the respondents are to be collected by use of a respondent agency. Moreover, a professional survey building, and collecting tool was made available for this research by the University of Twente. For the non-user and user participant group to be comparable, the non-user participant group was educated by means of a three-minute manipulation video, shown to them prior to filling in the questionnaire. The video contained a brief introduction, and the positive and negative aspects of third-party tracking and TBPPT.

3.2 Procedure

To answer the research question this research will be tested against a sample of the Dutch population. The Netherlands is part of the European Union with a total of 95.7% Internet users on their total population (IWS, 2015). The Central Bureau of Statistics (CBS) reported that the Internet skills of the Dutch population are well above average compared to he rest of the European Union (2014). The large percentage of Internet users and skills suggest that most of the population is familiar with, or has been unconsciously victimized by third-party tracking.

There existed a total of three requirements for participating in this research. First of all, as the case study is of the Netherlands, the participants were required to be a present inhabitant of this same country. Second, that the participant can read and understand the Dutch language, as the measurement instrument is conveyed in this language. Third, that the participant is above 18 years of age, as permission to use the provided information needs to be given. There was no requirement imposed in regards to Internet use was given, as the questionnaire was solely distributed via e-mail and Social Media. Moreover, the data was collected using the online survey-building, distribution, and collection tool Qualtrics. It was therefore assumed that any participant could safely be considered an Internet user.

To ensure minimal translational bias for this research instrument, a back-translation technique was applied. The original instrument was first translated from the source language (English) to the target language (Dutch) by the researcher. Subsequently, the translated instrument was then translated back to the source language (English) by a bilingual native Dutch-speaking translator. The back-translated instrument was then compared by a third independent rater to root out and correct any inconsistencies found. Having ironed out any translational bias by means of back translation, a pre-test was held in order to identify any potential problems to the process of filling out the questionnaire. The pre-test was held among a sample consisting of Dutch students (n=11) aged 22 - 27 (M = 22, SD = 2.166) with a minimum of 8 years of Internet experience. A separate pilot test was done for the non-user manipulation video. Participants were requested to view the video and report back any unclear aspects of it. Based on the feedback received any errors and unclear aspects were altered.

Data collection lasted from 24 April until 15 May 2015 and the responses were gathered using the services of Respondentedatabase.nl.

3.2 Participants

All participants were obtained by means of the participant-facilitating agency Respondentennet.nl. A total of 580 participants were collected. Out of these 580 participants, 444 participants were users, and 136 participants were non-users. To improve the reliability of these responses three filters were applied to weed out bad responses. The data set was tested against whether participants had completely finished the questionnaire, in what time frame the questionnaire was filled in, and whether there was suspicion of straightlining.

Table 1

Demographics

Demographic characteristics	Min	Max	M	SD
Age[b)]	19	82	47.75	15.00
Age[c)]	18	80	48.00	14.91
	Frequency[b)]	Percentage[b)]	Frequency[c)]	Percentage[c)]
Gender				
Male	44	47.31	130	54.17
Female	49	52.69	110	45.83
Education				
Primary school	0	0	1	0.42
High school	18	19.35	43	17.92
Practical education	38	40.86	87	36.25
Bachelor	32	34.41	79	32.92
Master	5	5.38	26	10.83
Other	0	0	4	1.67
Occupation				
Student	11	11.83	18	7.50
Employed	45	48.39	108	45.00
Self-employed	5	5.38	13	5.42
Unemployed	7	7.53	31	12.92
Retired	13	13.98	39	16.25
Other	12	12.90	31	12.92
Total	93	100	240	100

[b)] non-users, [c)] users

After removing unreliable responses form the data set a total of 458 respondents remained. Participants were divided in one of three groups: the non-users, users who use browser settings, and users who use either browser add-ons or software. After reviewing the data, it was decided to exclude the browser settings participant group, as it could not be determined whether this participant group adopted TBPPT to protect themselves from third-party tracking, or for unidentifiable reasons.

The non-users group consisted of 90 participants (47.3% male; age; M = 47.75, SD = 15.00; range 19–82 years), and the users who employ either browser add-ons or software contained 236 participants (54.2% male; age; M = 48.00, SD = 14.91; range 18-80 years). The demographics between the two participant groups appear to be similarly distributed (see Table 1). The only notable differences exist in the higher percentage of men in the Software and add-on users (male; NU 47,31%; U 54,17%), and the lower percentage of NU participants who have achieved a master's degree (Master; NU; 5,38%; U 10,83%). Surprisingly, user participant group turned out to be the largest of the three participant groups

(see Table 1). Moreover, a majority of the users is using TBPPT software to protect their online privacy (n = 195; 81,25%) over browser add-ons (n = 45; 18,75%).

3.3 Measurements

The questionnaire started with an introductory text, briefly introducing the author, elaborate on the research and its goals and on what is expected of the participant. The participant was then requested to confirm to have read and understood the text and conditions it posed.

Following the introductory text the questionnaire split the respondents into users and non-users of TBPPT. This was done by means of the provision of a definition of TBPPT and a question asking whether the respondent used TBPPT or not. Subsequently demographic factors were asked such as age, sex, province education, and employment and Internet usage. Participants who were classified as non-users were required to watch a tracking education video of three minutes before being able to progress to the attitude measurement scales.

Following the demographics participants were presented a total of 10 7-point Likert-style attitude measurement scales of which each contained 4-7 items, which are presented below in Table 2.

Table 2

Scales used in Questionnaire

Code	Items
Perceived Severity (SEV) (Mohamed & Ahmad, 2012; Woon, Tan & Low, 2005*)	
SEV1	Losing personal information privacy through browsing the Internet would be a serious problem for me.
SEV2	Having personal identifiable information (name, address, e-mail address, phone number, social security number) collected while browsing the internet would be a serious problem for me.
SEV3	Having non-personal identifiable information (browsing behaviour, time on a page, what page is visited next, interests, hobbies, search history) collected while browsing the internet would be a serious problem for me**.**
SEV4	Advertisement networks collecting my personal information and creating a profile based on my browsing behaviour is a serious problem for me.
SEV5*	Loss resulting from tracking my internet browsing is not a serious problem for me.
Perceived Vulnerability (VUL) (Dinev & Hart, 2004)	
VUL1	Personal information could be sold to third parties.
VUL2	Personal information collected could be misused.
VUL3	Personal information could be made available to unknown individuals or companies without my knowledge.
VUL4	Personal information could be made available to government agencies.
VUL5	Personal information could be inappropriately used.
VUL6	Unethical use of collected information is attractive to some companies.
VUL7	Legal but questionable use of collected information is profitable to some companies.
Intrinsic rewards (IRW) (self-developed scale)	
Online personalized advertisements…	
IRW1	allow me the opportunity to save time when I shop online.
IRW2	make it easier for me to find products or services that I need.

IRW3	make me conscious of products or services that I might need, but was not aware of.
IRW4	have my preferences over traditional mass marketing, as they only show relevant products and services.
Extrinsic rewards (ERW) (self-developed scale)	
I would allow the tracking of my personal information and the showing of advertisements while I browse the Internet if…	
ERW1	I would support the websites I visit by doing so.
ERW2	I would help my favorite websites to continue existing.
ERW3	this would increase the quality of my favorite websites.
ERW4	I would help maintain the quality and content of the Internet by doing so.
Performance expectancy (PE) (Venkatesh, et al. 2003)	
PE1	I would find the system useful in my job.
PE2	Using the system enables me to accomplish tasks more quickly.
PE3	Using the system increases my productivity.
PE4	If I use the system, I will increase my chances of getting a raise.
Effort expectancy (EE) (Venkatesh, et al. 2003)	
EE1	My interaction with the system would be clear and understandable.
EE2	It would be easy for me to become skillful at using the system.
EE3	I would find the system easy to use.
EE4	Learning to operate the system is easy for me.
Response costs (RC) (Woon, Tan & Low, 20005)	
RC1	The cost of enabling technology-based privacy protection tools would decrease the convenience afforded by browsing the Internet.
RC2	There are too many overheads associated with trying to enable technology-based privacy protection tools on an Internet browser.
RC3	Enabling technology-based privacy protection tools on an Internet browser would be time consuming.
RC4	Enabling technology-based privacy protection tools on my internet browser would require considerable investment of effort other than time.
Facilitating conditions (FC) (Venkatesh et al., 2003)	
FC1	I have the resources necessary to use the system.
FC2	I have the knowledge necessary to use the system.
FC3	The system is not compatible with other systems I use.
FC4	A specific person (or group) is available for assistance with system difficulties.
Social influence (SI) (Venkatesh, et al. 2003)	
SI1	People who influence my behaviour think that I should use the system.
SI2	People who are important to me think that I should use the system.
SI3	The senior management of this business has been helpful in the use of the system.
SI4	In general, the organization has supported the use of the system.
Behavioral intention (BI) (Kumar et al., 2008)	
BI1	I intend to engage in technology-based privacy protection in the next three months.
BI2	I predict that I would engage in technology-based privacy protection in the next three months.
BI3	I plan to engage in technology-based privacy protection in the next three months.
System usage (USE) (Lucas & Spitler, 2000*)	
USE1	How often do you use technology-based privacy protection tools?
USE2	How frequent do you use technology-based privacy protection tools?
USE3*	At the present time, I consider myself to be an extremely frequent user of technology-based privacy protection
USE4*	I currently use technology-based privacy protection continuously throughout the day

3.4 Measurement instrument reliability

The test of multicollinearity was applied to the data (see Table 3). There are many "rules of thumb" which guide the researcher on how to interpret the variance inflation factor and tolerance level, the most used appear to be a VIF of 10, 5, and 4 (Field, 2009). As the maximum variance inflation factor is 2.55, and the lowest level of tolerance .392, there is no reason to worry about multicollinearity in for this research (see Table 3).

Table 3
Collineary statistics for the factors predicting behavioral intention and system usage

Collinearity Statistics					
		Non-users Model		Users Model	
Dependent Variable	IV's	Tolerance	VIF	Tolerance	VIF
Perceived severity (SEV)	VUL	.869	1.151	.924	1.082
	IRW	.689	1.451	.664	1.507
	ERW	.644	1.553	.597	1.674
	PE	.520	1.922	.493	2.030
	EE	.505	1.982	.441	2.269
	RC	.933	1.072	.808	1.238
	FC	.669	1.495	.393	2.543
	SI	.714	1.400	.827	1.210
Perceived vulnerability (VUL)	SEV	.543	1.840	.812	1.232
	IRW	.664	1.505	.663	1.509
	ERW	.579	1.726	.590	1.694
	PE	.503	1.987	.490	2.042
	EE	.502	1.993	.443	2.258
	RC	.896	1.116	.776	1.288
	FC	.657	1.521	.392	2.550
	SI	.666	1.503	.803	1.246
Intrinsic rewards (IRW)	SEV	.542	1.845	.812	1.232
	VUL	.835	1.197	.923	1.084
	ERW	.694	1.441	.770	1.299
	PE	.442	2.264	.485	2.060
	EE	.521	1.920	.441	2.269
	RC	.899	1.112	.776	1.288
	FC	.663	1.507	.392	2.552
	SI	.707	1.415	.829	1.206
Extrinsic rewards (ERW)	SEV	.586	1.707	.830	1.205
	VUL	.842	1.187	.934	1.071
	IRW	.803	1.246	.874	1.144
	PE	.441	2.265	.499	2.003
	EE	.562	1.780	.464	2.156
	RC	.943	1.060	.822	1.216
	FC	.688	1.453	.392	2.552
	SI	.667	1.500	.799	1.251
Performance expectancy (PE)	SEV	.612	1.635	.820	1.220
	VUL	.946	1.057	.928	1.078
	IRW	.660	1.515	.661	1.514
	ERW	.571	1.753	.598	1.671
	EE	.586	1.707	.473	2.116
	RC	.901	1.110	.777	1.287
	FC	.659	1.518	.454	2.202
	SI	.685	1.461	.811	1.232

Effort expectancy (EE)	SEV	.523	1.912	.808	1.238
	VUL	.831	1.203	.925	1.081
	IRW	.686	1.457	.661	1.514
	ERW	.640	1.562	.612	1.633
	PE	.517	1.935	.520	1.921
	RC	.910	1.099	.783	1.277
	FC	.718	1.393	.532	1.880
	SI	.665	1.504	.824	1.213
Response costs (RC)	SEV	.542	1.845	.841	1.190
	VUL	.832	1.202	.920	1.087
	IRW	.664	1.505	.661	1.514
	ERW	.602	1.660	.616	1.623
	PE	.445	2.246	.486	2.058
	EE	.510	1.961	.445	2.249
	FC	.658	1.520	.397	2.518
	SI	.671	1.489	.827	1.209
Facilitating conditions (FC)	SEV	.528	1.893	.812	1.231
	VUL	.830	1.205	.923	1.084
	IRW	.666	1.500	.662	1.511
	ERW	.598	1.672	.583	1.716
	PE	.443	2.258	.564	1.774
	EE	.547	1.828	.600	1.668
	RC	.894	1.118	.788	1.269
	SI	.666	1.501	.808	1.238
Social influence (SI)	SEV	.557	1.794	.837	1.195
	VUL	.830	1.204	.926	1.080
	IRW	.701	1.426	.687	1.457
	ERW	.572	1.748	.583	1.717
	PE	.455	2.200	.494	2.026
	EE	.501	1.998	.455	2.196
	RC	.902	1.108	.805	1.243
	FC	.658	1.520	.396	2.526

3.5 Factor analysis

Using orthogonal rotation (varimax) the rotated component matrix shows the factor loadings for each variable into each factor. Loadings below the criterion value of 0.4 have been suppressed for interpretive purposes (Field, 2009). Looking at the content of each of the three rotated component matrixes, it can be seen that for the non-users SI loaded two items into perceived severity (see Table 4), though not sufficient enough to worry. For the user participant group however, the items of both EE and FC appear to have loaded into Factor 1 (See Table 5). This suggests that either one of the scales failed to measure what it was intended for, or that the items are sub-components of EE (Field, 2009,).

To test whether or not the items of EE and FC truly are loaded into the same factor, thereby suggestion that they are measuring the same, a separate factor analysis was done including only the items of EE and FC for the dataset of the user participant group. From the separate factor analysis it can be interpreted that the items of EE and FC do load separately and therefore neither component will be removed from this research and used for further data analysis (see Table 6).

Table 4
Rotated Component Matrix Non-users

	1	2	3	4	5	6	7	8	9	10
VUL1	0.81									
VUL2	0.89									
VUL3	0.93									
VUL4	0.89									
VUL5	0.92									
VUL6	0.62									
VUL7	0.77									
SEV1		0.84								
SEV2		0.93								
SEV3		0.82								
SEV4		0.91								
SEV5		0.88								
IRW1					0.77					
IRW2					0.86					
IRW3					0.85					
IRW4					0.79					
ERW1				0.86						
ERW2				0.89						
ERW3				0.90						
ERW4				0.83						
EE1							0.79			
EE2							0.78			
EE3							0.76			
EE4							0.76			
PE1			0.82							
PE2			0.82							
PE3			0.82							
PE4			0.84							
SI1		0.46								0.56
SI2		0.47								0.59
SI3										0.86
SI4										0.81
FC1									0.77	
FC2									0.73	
FC3									0.74	
FC4									0.63	
RC1						0.70				
RC2						0.90				
RC3						0.90				
RC4						0.89				
BI1								0.83		
BI2								0.91		
BI3								0.92		

Extraction Method: Principal Component Analysis

Rotation Method: Varimax with Kaiser Normalization

a Rotation converged in 8 iterations,

Table 5
Rotated Component Matrix Users

	1	2	3	4	5	6	7	8	9
VUL1		0.78							
VUL2		0.78							
VUL3		0.89							
VUL4		0.88							
VUL5		0.89							
VUL6		0.76							
VUL7		0.74							
SEV1			0.81						
SEV2			0.83						
SEV3			0.74						
SEV4			0.87						
SEV5			0.85						
IRW1					0.89				
IRW2					0.88				
IRW3					0.88				
IRW4					0.83				
ERW1						0.84			
ERW2						0.87			
ERW3						0.88			
ERW4						0.85			
EE1	0.79								
EE2	0.91								
EE3	0.87								
EE4	0.90								
PE1									0.62
PE2	0.47								0.66
PE3	0.49								0.57
PE4									0.66
SI1							0.86		
SI2							0.89		
SI3							0.90		
SI4							0.87		
FC1	0.58			0.47					
FC2	0.75								
FC3	0.56			0.47					
FC4	0.57								
RC1								0.77	
RC2								0.87	
RC3								0.87	
RC4								0.84	
USE1				0.75					
USE2	0.46			0.74					
USE3				0.76					
USE4				0.74					

Extraction Method: Principal Component Analysis,

Rotation Method: Varimax with Kaiser Normalization,

a Rotation converged in 8 iterations,

Table 6
Rotated Component users EE and FC Users

	1	2
EE1	0.800	
EE2	0.877	
EE3	0.874	
EE4	0.891	
FC1		0.798
FC2	0.527	0.672
FC3		0.842
FC4		0.760

Extraction method: Principal Component Analysis
Rotation method: Varimax with Kaiser Normalization
a Rotation converged in 3 iterations,

3.6 Cronbach's Alpha

In order to test the reliability of the measurement instrument Cronbach's Alpha was conducted on the scales. Table 7 presents the results.

Table 7
Descriptive Statistics

Measurement Scales	Items[b)]	a[b)]	M[b)]	SD[b)]	Items[c)]	a[c)]	M[c)]	SD[c)]
Perceived vulnerability	7	0.93	5.35	1.33	7	0.92	5.45	1.28
Perceived severity	5	0.95	4.78	1.45	5	0.92	4.89	1.17
IRW?	4	0.89	3.92	1.25	4	0.94	3.73	1.61
ERW?	4	0.95	4.21	1.40	4	0.96	3.45	1.56
Effort expectancy	4	0.91	4.65	1.15	4	0.93	4.77	1.22
Performance expectancy	4	0.96	5.13	1.12	4	0.92	5.48	0.91
Social influence	4	0.84	4.07	1.25	4	0.91	4.56	1.43
Facilitating conditions	4	0.84	4.54	1.09	4	0.87	5.20	0.97
Response costs	4	0.88	4.09	1.06	4	0.89	3.88	1.25
Behavioral intention	3	0.97	3.47	1.58				
System usage					4	0.90	5.29	1.09

[b)] non-users, [c)] users
Note: constructs were measured on a 7-point Likert scale (1 = totally disagree/7 = totally agree)

In order to ensure high reliability of the measurement instrument existing, and proven to be reliable scales were used and altered to befit this research. As can be seen form Table 7, the lowest alpha for either participant group is .84. The threshold for an acceptable alpha is generally put at .7 (Cortina, 1993). As all of the scales score well above and beyond that threshold, it can be assumed that the scales are sufficiently reliable.

Section 4: Results

4.1 Correlational analysis

A bivariate correlational analysis in the form of Pearson's product-moment coefficient was conducted on the data sets to investigate whether any of the variables co vary, and to quantify the strength of the relationship between these variables (Field, 2009). Pearson's product-moment coefficient presents a table where the variables are given values ranging between -1 and +1, where 0 to -1 stands for a negative correlation, and 0 to +1 stands for a positive correlation. The closer to 0 the value is, the less strong its correlation is to the paired variable. A commonly used measure is for ± .1 to be considered a small effect, ± .3 to be a medium effect and ± .5 to be a large effect (Field, 2009).

4.1.1 Non-users

Table 8 presents the results of the Pearson's product-moment coefficient applied to the non-user data set. A total of five variables appear to have a significant correlation when paired to the dependent variable behavioural intention. Most notable is social influence (r = .464) which holds the highest correlational effect, and perceived severity (r = .401), intrinsic rewards (r = .383) and facilitating conditions (r = .368), which all can be considered to have a medium-sized correlational effect on behavioural intention. Other variables that have a small correlational effect on behavioural intention are performance expectancy (r = .239) and effort expectancy (r = .208).

Table 8
Correlations Matrix Non-users

Construct	VUL	SEV	IRW	ERW	EE	PE	SI	FC	RC	BI
Perceived vulnerability (VUL)										
Perceived severity (SEV)	.04									
Intrinsic rewards (IRW)	.03	.21*								
Extrinsic rewards (ERW)	-.02	-.06	.44**							
Effort expectancy (EE)	.17	.26*	.16	.39**						
Performance expectancy (PE)	.34**	.48**	.22*	.17	.58**					
Social influence (SI)	.05	.47**	.37**	.17	.24*	.38**				
Facilitating conditions (FC)	.06	.23*	.29**	.41**	.53**	.39**	.20			
Response costs (RC)	-.02	.10	.12	.17	-.05	.01	.13	.01		
Behavioral intention (BI)	.08	.40**	.38**	.08	.21*	.24*	.46**	.37**	-.01	

** Correlation significant at the .01 level (2-tailed)
* Correlation significant at the .05 level (2-tailed)

4.1.2 Users

Table 9 presents the results of Pearson's product-moment coefficient applied to the users data set. All but three variables appear to have a significant correlation with behavioural intention. Two very large correlational effects were found on behavioural intention, namely performance expectancy (r = .644) and facilitating conditions (r = .657). Other significant correlational effects were effort expectancy (r = .529) with a large correlational effect, perceived severity (r = 2.88) with a medium correlational effect, and perceived vulnerability (r = .154) and social influence (r = .167) with a small correlational effect.

Table 9
Correlations Matrix Users

Construct	VUL	SEV	IRW	ERW	EE	PE	SI	FC	RC	USE
Perceived vulnerability (VUL)										
Perceived severity (SEV)	.16*									
Intrinsic rewards (IRW)	-.03	-.11								
Extrinsic rewards (ERW)	-.16*	-.21**	.54**							
Effort expectancy (EE)	.02	.09	.09	.09						
Performance expectancy (PE)	.19**	.26**	-.04	-.18**	.56**					
Social influence (SI)	.13*	.23**	.22**	.11	-.04	.15*				
Facilitating conditions (FC)	.14*	.20**	.05	.-06	.69**	.66**	.10			
Response costs (RC)	-.05	.12	.17*	.26**	-.23**	-.21**	.23**	-.24**		
System Usage (USE)	.15*	.29**	-.05	-.06	.53**	.64**	.17**	.66**	-.13	

** Correlation significant at the .01 level (2-tailed)
* Correlation significant at the .05 level (2-tailed)

4.2 Regression analysis

As this research is based upon the UTAUT complemented with additional variables from the Protection Motivation Theory (PMT), a hierarchical regression was performed. As the Unified Theory of Acceptance and Use of Technology (UTAUT) is the core of this research, model 1 (see table 10) primarily consists of UTAUT the variables effort expectancy (EE), performance expectancy (PE), social influence (SI) and facilitating conditions (FC). Model 2 holds the additional PMT variables of perceived vulnerability (VUL), perceived severity (SEV), intrinsic (IRW) and extrinsic rewards (ERW), response costs (RC) and tests the model as a whole. Table 10 presents the findings form the non-users data.

4.2.1 Non-users

From Table 10 can be seen that a total of 30% (UTAUT: R2 = .30) variance on behavioural intention can be explained by the UTAUT variables, which increases by 9% (ΔR2 = .09) to 39% when the PMT variables are added (OPPM: R2 = .39). Furthermore, cross-validation has been tested through the adjusted R2, which shows that if the model had been tested against the population that the sample was taken from, 32% (model 2: Adj. R2 = .32) variance on behavioural intention would be accounted for.

The non-users participant group has a total of three variables significantly predicting BI; SI (β = .31, p = < .01), FC (β = ..30, p = < .01), and IRW (β = .25, p = < .01). Contrary to its expectations, IRW has been identified as significant positive predictor of BI. This causes H8a and H9a to be supported, and H3a to be rejected. Another interesting result is though insignificant, PE function as a negative predictor (β = -.16) on BI. The remaining variables of EE, VUL, SEV, ERW and RC all function in the predicted direction yet have been found insignificant, rejecting H1a, H2a, H4a, H5a, H6a and H7a.

Table 10

Hierarchical regression on behavioral intention for the non-users' model

Regression Coefficients						
Models	B	SE B	b	R^2	Adj. R^2	ΔR^2
Model 1				**.30**	**.26**	
Constant	-.34	.79				
Effort expectancy	-.07	.16	-.01			
Performance expectancy	-.02	.16	-.00			
Social influence	.53	.12	.42***			
Facilitating conditions	.45	.15	.31**			
Model 2				**.39**	**.32**	**.09**
Constant	-.67	1.0				
Effort expectancy	.04	.17	.03			
Performance expectancy	-.22	.18	-.16			
Social influence	.39	.13	.31**			
Facilitating conditions	.43	.16	.30**			
Perceived vulnerability	.09	.11	.08			
Perceived severity	.22	.12	.20			
Intrinsic rewards	.32	.13	.25**			
Extrinsic rewards	-.19	.13	-.17			
Response costs	-.10	.13	-.07			

*** p < .001, ** p < .01, * p < .05

4.2.2 Users

Table 11 holds the results of hierarchal regression analysis for the user participant group. The results show that for the UTAUT variables 52% (model 1: R2 = .52) variance can be explained in relation to behavioural intention, which increases by 2% (ΔR2 = .02) when the PMT variables are added to the model (model 2: R2 = .54). Cross-validation by means of the adjusted R2 showed that the predicted power of the OPPM will only shrink by a minimum of 2% (Adj. R2 = .52) when tested against the population that the sample was taken from.

Model 2 holds four significant predictors of behavioural intention, namely PE (β = .32, p = < .001), FC (β = .36, p = < .001), SEV (β = .10, p = < .05) and IRW (β = .12, p = < .05). This leads to the support of H1a, H3a, H6a, and H9a. EE, SI, VUL, ERW and RC were found to be insignificant predictors of BI, leading to the rejection of H2a, H4a, H5a, H7a and H8a. Though non-significant, ERW and RC were found to relate to BI in the opposite hypothesized direction than suspected.

Table 11

Hierarchical regression on behavioral intention for the users' model

Regression Coefficients						
Models	B	SE B	b	R^2	Adj. R^2	ΔR^2
Model 1				**.52**	**.51**	
Constant	.24	.34				
Effort expectancy	.08	.06	.09			
Performance expectancy	.41	.07	.34***			
Social influence	.06	.04	.08			
Facilitating conditions	.41	.08	.36***			
Model 2				**.54**	**.51**	**.02**
Constant	-.20	.45				
Effort expectancy	.09	.06	.10			
Performance expectancy	.39	.08	.32**			
Social influence	.05	.04	.07			
Facilitating conditions	.40	.08	.36***			
Perceived vulnerability	.02	.04	.03			
Perceived severity	.10	.05	.10*			
Intrinsic rewards	-.08	.04	-.12*			
Extrinsic rewards	.06	.04	.08			
Response costs	.02	.04	.02			

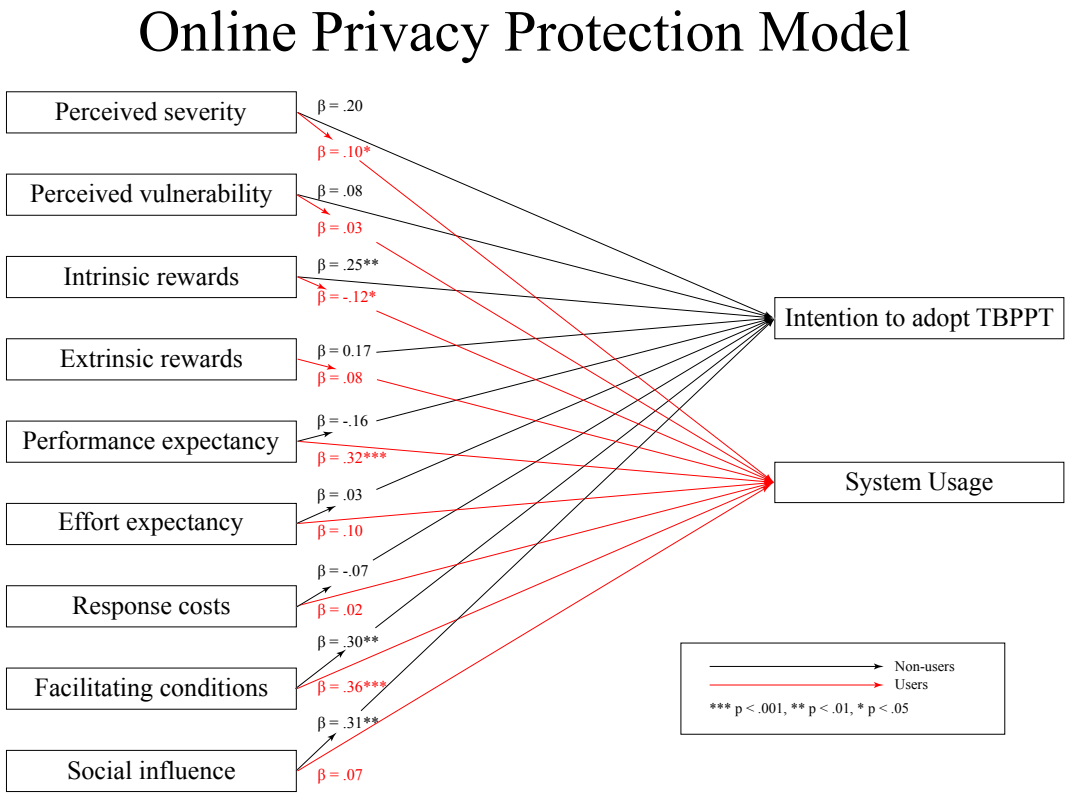
*** p < .001, ** p < .01, * p < .05

5. Discussion

5.1 Evaluation of the Online Privacy Protection Model

By the testing of the Online Privacy Protection Model against the research question of "What factors influence the decision of Internet users' to adopt and use technology-based privacy protection tools?" this research has identified seven significant predictors of the adoption of technology-based privacy protection tools (TBPPT) (see Figure 2). From the two participants groups the non-users group found that social influence (SI), facilitating conditions (FC) and intrinsic rewards (IRW) are significant predictors of the intention to adopt TBPPT. The users participant group found a total of four significant predictors: performance expectancy (PE), facilitating conditions (FC), perceived severity (SEV), and intrinsic rewards (IRW). The discussion section will further discuss the results, its practical implications, theoretical relevance, limitations, and conclude upon this research.

Figure 2:



5.1.1 Non-users

For the non-users there were three significant predictors on behavioural intention (BI), namely social influence (SI), facilitating conditions (FC), and intrinsic rewards (IRW). As hypothesized based upon existing literature, SI and FC were found to be statistically significant predictors of BI. These results make sense as those who do not use technology-based privacy protection tools (TBPPT) will most likely be made aware of the threat of third-party tracking by their peers. Subsequently, the findings suggest that non-users have a social environment that supports the use of TBPPT. As for FC, non-users will most likely affix more value to the available FC due to their inexperience with the TBPPT.

The significant positive result of IRW was surprising, as the opposite relation was hypothesized. In a study examining user concerns for online tracking and advertising, Agarwal et al., (2013) reported that Internet users did not mind the personalization of advertisements as much as they were annoyed with embarrassing, or repetitive advertisements. Moreover, a situational bias was reported on in regards to third-party tracking, where only sensitive topics (such as banking) were frowned upon, and a more neutral attitude was in place towards third-party tracking in general, though found to be highly varying. This could explain why a significant positive relationship exists between IRW and BI.

Although hypothesized as expected to be significant, the non-users participant group had six insignificant predictors of BI, namely effort expectancy (EE), performance expectancy (PE), perceived vulnerability (VUL), perceived severity (SEV), extrinsic rewards (ERW), and response costs (RC). The insignificant result of both PE and EE on BI could be explained by the significant result of SI. When a non-user gets introduced to the landscape of third-party tracking and TBPPT, they might not base their decisions whether or not to use TBPPT on the expected performance or required effort, but on the advice and support of the person who introduced them. Furthermore, there are the insignificant predictors of VUL and SEV, which suggests that the non-users do not find the VUL and SEV of third-party tracking sufficient to engage in the use of TBPPT. The insignificant result of ERW signifies that even though third-party tracking and online behavioural advertising (OBA) can be considered part of the Internet eco-system, it is insufficient reason to engage in the use of TBPPT. Reasoning for this result could potentially be that Internet user's do not assess the trade-off of the content, services, or products that the website is offering as valuable enough to give up their personal information. Lastly, RC failing to be a significant predictor of BI might be as non-users have yet to experience the usage of TBPPT first-hand themselves, and might therefore not be sufficiently familiar with the potential hindrances that TBPPT might cause. Although educated on the potential RC they might not fully understand what the RC of TBPPT entail, and how it affects the convenience of browsing the Internet.

5.1.2 Users

As for the users participant group, four variables were found to significantly predict system usage, namely PE, FC, SEV, and IRW. The significant result of performance expectancy implies that the TBPPT users find it essential for a TBPPT to match the performance expected to start, and keep using it. Similar to PE, FC is a core variable of the UTAUT and its significance show that TBPPT users find it imperative that there exists support system surrounding the TBPPT. The combination of a significant result for SEV, and an insignificant result for VUL, implies that TBPPT users find the practice of third-party tracking sufficiently severe to worry about, yet an insignificant result of VUL suggests that the probability of occurrence to themselves specifically, is not. A potential explanation for these specific results could be optimistic bias. In a study about optimistic bias about online privacy risks, Hichang, Jae-Siyoung, and Siyoung (2010) found that Internet users "judge themselves to be significantly less likely than others to experience online privacy risks (p. 992)." The outcome of IRW to be a significant negative predictor of BI was as hypothesized. However, when viewing the result of IRW next to that of ERW, it can be contemplated that the TBPPT user engages in TBPPT due to direct and personal gain, over ethical reasoning.

EE, SI, RC were all found to be insignificant predictors of BI. The insignificant result of EE could be attributed to the characteristics of the TBPPT users group. As the users participant group consists of users who are all experienced in both Internet usage, and TBPPT usage and could therefore consider engaging in TBPPT not to be a task, which would take a great amount of effort (Zhou, 2012). As the user participant group already are TBPPT users, it might explain why SI was deemed insignificant as a predictor of BI. Judging from the large amount of long-term TBPPT users SI might not hold sufficient value to be a significant

predictor. This finding is consistent with the results of Yun, Han, and Lee (2013) who found that SI did not have a significant effect on continuous usage intention. The insignificant result of the RC of TBPPT on USE could be attributed to the experience the users participant group have with TBPPT. Perhaps the TBPPT users have gotten used to the RC of TBPPT to such an extent that they do not even realize the RC anymore, or at least are not as bothered by it.

5.2 Practical implications

This research has presented a potential method to either get Internet users to use TBPPT, or to maintain their usage. To motivate Internet users to use TBPPT it is imperative that the social environment is supportive of the usage of TBPPT. Meaning that new TBPPT are best recruited through the social network of current users. Developers of TBPPT could exploit this finding in their attempt to acquire new users by trying to tap into the network of the current users. Encouragement of endorsing the TBPPT could be rewarded by a discount, or allowing the usage of special features.

Furthermore, the FC hold weight in user acceptance as well. This finding suggests that potential users of TBPPT hold value to the extend of available support and service for the TBPPT. TBPPT developers could apply the significant result of FC by emphasizing supportive and service-related features that come with the TBPPT. Examples could be an option for guidance or any questions (non-)users might have by phone, email, or chat , a FAQ section on the website, or guides on how to install and use the TBPPT in question.

Based on the results of this research the current users of TBPPT hold different expectations and requirements to TBPPT for continuous usage than non-users. The strongest among the factors affecting continuous usage being PE and FC, suggesting that as expertise with TBPPT rises, the requirements put to the TBPPT does so as well. Furthermore, SEV and IRW are found to be significant predictors of the continuous usage as well. The SEV and IRW variables complement the significant result of PE in terms of practical implications, as the Internet user assesses PE by means of the ability of the TBPPT to nullify the SEV and OBA threat. TPBBT developers could use this finding in their promotional efforts by accentuating how the TBPPT will help the TBPPT user excel in protecting their online privacy. Focus areas in these promotional efforts should be how the TBPPT would address and prevent the threat of both SEV, and OBA. As with the non-users participant group, the TBPPT users attach value to available FC supplemented by the TBPPT, the same advice holds for the FC results of the users.

5.4 Theoretical relevance

The merger of the UTAUT and PMT into the Online Privacy Protection Model has been shown as relevant by this research. Whereas the UTAUT has been argued to lack context (Venkatesh, Thong, Chan, Hu, & Brown (2011), and the PMT has been designed primarily for a health-related context, the OPPM has combined the two, in an attempt to explore what factors influence Internet users to adopt TBPPT. Although not all the variables were found to be significant predictors of BI or USE, the non-users and users group were found to have significant predictors from both models. By identifying variables that successfully and fail to predict BI and USE of TBPPT, this study has offered the basis for the a new privacy-related technology acceptance model.

Potential improvement of the model could be achieved when limitations from this research were to be addressed. For example, even though a video-balance test was used for the tracking & TBPPT educational video for the non-users participant group, it might influence

participants in manners not intended. Some might consider the video unprofessionally made, too fast, too long, or do not like the speakers voice. Furthermore, the participant groups were not divided equally, resulting in a non-users group of 90 participants, and a users group of 236 participants. Lastly, the exclusion of certain PMT variables over UTAUT variables might have influenced the results, using self-efficacy or response-efficacy over its UTAUT counterparts could potentially result in more significant outcomes. Potentially more interesting results could be achieved if these limitations were not present.

5.5 Conclusion

Having identified, tested, and reported on the predictors of user acceptance of TBPPT, this research has presented the Online Privacy Protection Model for the explaining the intention to adopt TBPPT. Although the TBPPT users model accounts for about 50% variance and 32% for the non-users, it has identified social influence, performance expectancy, facilitating conditions, perceived severity, and intrinsic rewards as predictors of the intention to adopt TBPPT. Future research should focus on eliminating the limitations and irrelevant variables used in this research, as well as identify new variables that could potentially add to this model. To conclude, this research has provided the basis for a model that has the potential of evolving into a theory that can be widely used to explain the user acceptance of technology-based privacy protection tools, in a digital landscape where the topic of online privacy is becoming ever more important.

Reference list

Agarwal, L., Shrivastava, N., Jaiswal, S. & Panjwani, S. (2013). Do not embarrass: Re-examining user concerns for online tracking and advertising. *Symposium on Usable Privacy and Security (SOUPS)* 2013, July 24-26, Newcastle, UK.

Casey, T. & Wilson-Evered, E. (2012). Predicting uptake of technology innovations in online family dispute resolution services: An application and extension of the UTAUT. *Computers in Human Behavior*, 28, 2034-2045. doi: 10.1016/j.chb.2012.05.022.

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on Systems Sciences*, 1-10.

Cho, H., Lee J. & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior* 26, 987-995. doi: 10.1016/j.chb.2010.02.012.

Cortina, J. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, 78(1), 98-104.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *2010 43rd Hawaii International Conference on System Sciences*, 1-10.

Dinev, T. & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behaviour & Information Technology*, 23 (6), 413-422. doi: 10.1080/01449290410001715723.

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

Field, A. (2009). *Discovering Statistics Using SPSS* (3rd ed.). Sage Publications.

Floyd, D. L., Prentice-Dunn, S. & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30 (2), 407-429.

Hallinan, D., Friedewald, M. & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28, 263-272. doi: 10.1016/j.clsr.2012.03.005.

Hsu, C. & Lee, M. (2013). User acceptance of a community-based healthcare information system preserving user privacy. *Universal Access in Human-Computer Interaction. Springer-Verlag Berlin Heidelberg* 2013, 453-462.

Im, I., Hong, S. & Kang, M. S. (2011). An international comparison of technology adoption testing the UTAUT model. *Information & Management*, 48, 1-8. doi: 10.1016/j.im.2010.09.001.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B. & Greer, C. (2013). Information disclosure on mobile services: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, 71, 1163-1173. Doi: 10.1016/j.ijhcs.2013.08.016.

Kumar, N., Mohan, K. & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision Support Systems, 46, 254-264. doi: 10.1016/j.dss.2008.06.010.

Lee, D., Larose, R. & Rifon, N. (2008). Keeping our network safe: A model of online protection behavior. *Behavior & Information Technology*, 27(5), 445-454. doi: 10.1080/01449290600879344.

Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, 32-44. doi: 10.1016/j.elerap.2013.08.002.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57, 343-354. doi: 10.1016/j.dss.2013.09.018.

Liao, C., Liu, C. & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, 10, 702-715. doi: 10.1016/j.elerap.2011.07.003.

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29, 1649-1656. Doi: 10.1016/j.chb.2013.01.049.

Lucas, H. C. & Spitler, V. (2000). Implementation in a world of workstations and networks. *Information & Management*, 38, 119-128.

Luo, X., Li, H., Zhang, J. & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, 49, 222-234. doi: 10.1016/j.dss.2010.02.008.

MacDonell, K., Chen, X., Yan, Y., Li, F., Gong, J., Sun, H., Li, X. & Stanton, B. (2013). A protection motivation theory-based scale for tobacco research among Chinese youth. *Addiction Research & Therapy*, 4 (3), 1-7. doi: 10.4172/2155-6105.1000154.

Maddux, J. E. & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19, 469-479.

Martins, C., Oliveira, T. & Popovic, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application.

International Journal of Information Management, 34, 1-13. doi: 10.1016/j.ijinfomgt.2013.06.002.

Mohamed, N. & Ahmad, I. H. (2012) Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28, 2366-2375. doi: 10.1016/j.chb.2012.07.008.

Sun, Y., Wang, N., Guo, X. & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *Journal of Electronic Commerce Research*, 14 (2), 183-200.

Udo, G., Bagchi, K. & Maity, M. (2014). Exploring factors affecting digital piracy using the norm activation and UTAUT models: The role of national culture. *Journal of Business Ethics, Spinger Science+Business Media Dordrecht*. doi: 10.1007/s10551-014-2484-1.

Venkatesh, V. & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273-315.

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hu, P. J. & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal*, 21, 527-555. Doi: 10.1111/j.1365-2575.2011.00373.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27 (3), 425-478.

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, 12 (4), 324-333.

Woon, I., Tan, G. & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*. Paper 31.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs*, 43(3), 389-418.

Yun, H., Han, D. & Lee, C. C. (2013). Understanding the use of location-based service application: Do privacy concerns matter? *Journal of Electronic Commerce Research*, 14(3), 215-230.

Zhang, L. & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8, 180-197. doi: 10.1080/15332860903467508.

Zhou, T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research*, 13(2), 135-144.

Zhou, T., Lu, Y. & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, 26, 760-767. doi: 10.1016/j.chb.2010.01.013.