Privacy for Burdened Minds

Exploring the Effects of Online Privacy Trade-offs on Cognitive Bandwidth

Wouter Moraal[1]

Graduation Thesis

Thesis advisors: Max van Duijn[1] and Hadi Asghari[2]

[1] Leiden University, Leiden Institute of Advanced Computer Science, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands
[2] TU Delft, Faculty of Technology, Policy and Management, Jaffalaan 5, 2628 BX Delft, The Netherlands
research@woutermoraal.nl

Abstract. This research project has been trying to connect theories and findings from both the research on economic trade-offs and online privacy trade-offs. Within these fields it was found that monetary trade-offs can limit cognitive function under certain conditions, and that limited cognitive function can result in higher disclosure of personal information online. Thus, it is explored if online trade-offs involving privacy could result in a negative spiral of increasing privacy concerns, limited cognitive function and subsequently higher information disclosure, basically forming a 'privacy trap' alike the much discussed 'poverty trap'. Using an experimental approach it is explored how online privacy trade-offs are able to limit cognitive bandwidth and cause cognitive scarcity. The cognitive function of inhibitory control is used as a measurement of cognitive bandwidth. Data were collected using an online survey including a hypothetical scenario, several measurement scales and an embedded Simon task. Participants (n=104) could be classified into three groups: associates of a privacy advocacy group, a Bachelor of Arts class, and a mixed group of co-students, family and friends of the author. The results of the study show no significant effect of the hypothesized variables on cognitive bandwidth. However, age is found to negatively affect inhibitory control and positively affect privacy risk belief. Information sensitivity and personal experiences of privacy violation have a positive effect on risk belief. Risk belief positively affects willingness to pay for non-disclosure, i.e. the degree to which participants were willing to pay a hypothetical sum of money to protect their privacy. Belief of personal protection sufficiency seems to somewhat positively affect risk belief and willingness to pay. Additionally, mediatory relationships between certain variables were discovered. At a methodological level, this research indicates that willingness to pay could be used as an alternative measure to behavioural intention scales in online privacy trade-offs. Lastly, a few methodological improvements are recommended for future research into the aspects of online trade-offs involving privacy.

Keywords: Online Privacy Trade-offs, Cognitive Scarcity, Inhibitory Control, Information Sensitivity, Risk Belief.

1 Introduction

Many business models that are used by today's online commercial giants center around the use of user information to be able to most effectively and/or lucratively sell advertisements. Users in turn are often drawn to apps and online services such as Facebook, Google Calendar and YouTube for entertainment, to organise their lives and to socially connect to other people. As a result, internet users in particular are now confronted with choices about their privacy on a daily basis. The European Commission took note of this and a few years ago started the process of creating legislation to assure EU citizens would be given certain legal tools that they could use to make more informed choices and assert a little more power concerning the use of information that third parties have about them. The resulting General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) has been implemented in laws in all EU member states as of 25 May 2018. In short, this piece of legislation makes it easier for users of services and products to gain insight into which information is disclosed by themselves or extracted from them by companies. Also the ability for users to request removal or change of this data in certain circumstances is strengthened by the GDPR. Additionally, EU citizens can now obtain limited insight into how the personal details that they disclose are used by parties involved.

While the possibility of a degree of insight, as offered by the GDPR, can help some people to make more informed choices concerning their privacy, it is unlikely that more information about these companies' practices will result in people always making wiser privacy choices. This can be compared to the legislation that requires the prints on the packaging of foods to include a table with ingredients and the fat and sugar contents. While these tables are a minimal requirement to be able to make an informed decision about whether or not one would be well advised to consume a certain product, they do in practice not prevent a lot of people from consuming products that are too high on sugar and fat. First of all, the legislation does not prevent the rest of the packaging from showing pictures and misleading slogans about the food's benefits, while omitting its nuisances. Also, it has been suggested that many shoppers still choose unhealthy products in favor of others because they don't have a lot of money or time, are already thinking about the next

Graduation Thesis for the Media Technology MSc program, Leiden University. August 2018.

products that they have to find, or are otherwise distracted; which are all factors that may drain their cognitive abilities to consciously decide about the product at hand. In other words, because people are cognitively burdened with worries and thoughts about time and money management, they are less able to focus on their main task of making a choice (Dean, Schilbach, & Schofield, 2017; Banerjee & Mullainathan, 2008). They then end up just going with whatever is most easy to see and the most readily at hand. The products that are most visible and easy to reach in a supermarket are usually the most expensive products which also had most money spent on their attractive packaging.

This paper investigates whether decision-making involving online products and services may suffer from similar distractions and mental pitfalls. What is different between most online decision-making situations and those in supermarkets, is that many of the online decision-making situations involve a dimension of privacy. In the next paragraphs it is explored whether worries about privacy and thoughts about personal information management burden the mind similarly to financial thoughts and worries. And whether this burdening could equivalently force people into taking the easy decision (e.g. leave a box allowing for unnecessary collection of personal information ticked) instead of the optimal decision concerning privacy (e.g. unticking a box that would allow for unnecessary collection of information). In fact, it was recently demonstrated how Facebook, Google and Microsoft are actively making it cognitively hard and time consuming to choose the privacy-friendly option, by nudging users with certain interface designs (Forbrukerrådet, 2018).

Studies about privacy-related behaviour have shown that many people who express concerns about their privacy still share a lot of their private information online in practice. This seemingly contradictory phenomenon has been termed the ‘privacy paradox’ by the scientists first describing it (Kokolakis, 2017; Norberg, Horne, & Horne, 2007). To understand why many internet users choose to seemingly abandon their stated privacy concerns and make choices that require giving away sensitive personal information (Veltri & Ivchenko, 2017; Tufeckci, 2008), it may help to see information disclosure behaviour as a kind of economic trade-off (Kokolakis, 2017; Dienlin & Trepte, 2015).

In the field of economics the phenomenon described above has been studied in recent years. In particular how monetary scarcity (poverty) and its consequences can lay claim on cognitive resources, often called ‘cognitive bandwidth’, has been subject to research (Mani, Mullainathan, Shafir, & Zhao, 2013a; 2013b; Shafir & Mullainathan, 2013; Shah, Mullainathan, & Shafir, 2012; Dean et al., 2017; Banerjee & Mullainathan, 2008). In the literature of cognitive psychology ‘cognitive functions’, also called ‘executive functions’, are the mental processes, which stem from the pre-frontal cortex of the brain, and which are used to direct attention, perform conscious actions and handle information (Lezak, Howieson, Loring, & Fischer, 2004; Miller & Cohen, 2001; Jurado & Rosselli, 2007; Lyon & Krasnegor, 1996; Suchy, 2009; Diamond, 2013). Thus, cognitive functions are essential to decision-making (Dean et al., 2017). Cognitive bandwidth is basically taken to be the available cognitive resources at a given point. These resources can take a limited amount of load (Luck & Vogel, 1997; Baumeister, Bratslavsky, Muraven, & Tice, 1998; Baumeister, Vohs, & Tice, 2007; Baumeister & Heatherton, 1996; Baddeley & Hitch, 1974), hence the term ‘bandwidth’. Because of its limited capacity, cognitive bandwidth could be seen as the bottleneck in decision-making.

Cognitive bandwidth can be taxed by certain distracting factors, thus causing scarcity in available mental resources. This phenomenon has been termed ‘cognitive scarcity’ (Veltri & Ivchenko, 2017). Actually, a negative spiral has been theorized around cognitive scarcity and economic decision-making, which is called the ‘poverty trap’ (Dean et al., 2017; Banerjee & Mullainathan, 2008). The poverty trap can be summarised as follows: poverty will probably lead to cognitive scarcity, cognitive scarcity leads to poor decision-making, and poor decision-making may lead to more poverty.

Recent research into online information disclosure has uncovered that inducing different types of ‘cognitive scarcity’, makes people disclose considerably more information online (Veltri & Ivchenko, 2017). This would mean that if privacy trade-offs would be found to cause cognitive scarcity, they might also cause people to be distracted during those same or subsequent privacy trade-offs, which would result in them handing over more information then if they would not have been distracted. If continuing this scenario along the lines of the economic theory of the ‘poverty trap’, then if people hand over more information they might feel that their privacy is in danger, causing them to worry more during subsequent privacy trade-offs. This would in turn result in cognitive scarcity, and so on. Summarised, this would form a negative feedback loop of privacy similar to the ‘poverty trap’.

Therefore, the main question which this research project tries to answer is: does a ‘privacy trap’ exist? This paper focuses on the chain of events preceding cognitive scarcity which would subsequently cause increased information disclosure as found by Veltri and Ivchenko (2017). The model showing the area of interest in this paper is depicted in Figure 1. The following subquestions follow from this model:

1. Which factors influencing cognitive scarcity can be identified in online privacy decision-making situations?
2. What is the degree of influence that each of these factors have? In other words, under what circumstances and influences within online privacy decision-making processes is people’s cognitive bandwidth affected the most?

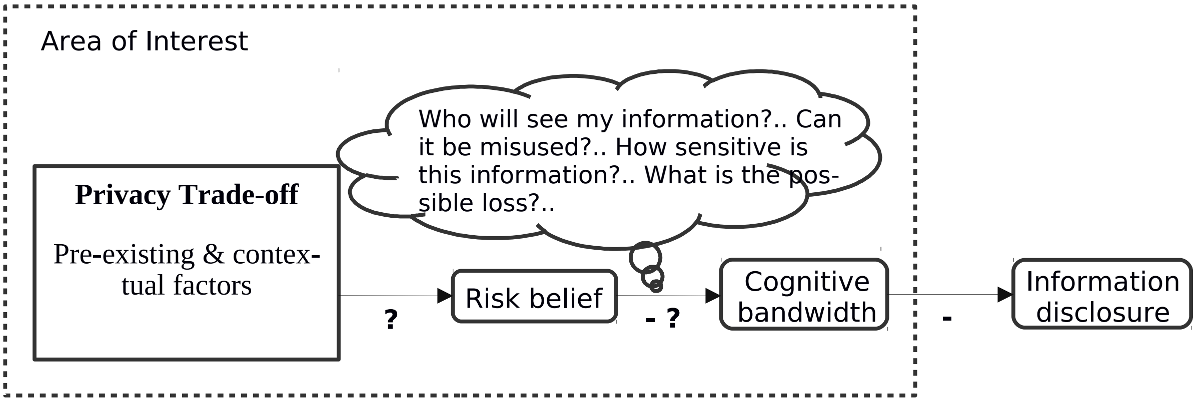

Fig. 1. Model showing the area of interest for this study and the relations therein to explore further.

In the remainder of this paper the answer to the two main research questions will be provided using the following structure. In Section 2 some more detail is given about the scientific field concerning the factors which might play an important role in privacy trade-offs influencing cognitive function. Additionally in this section the hypotheses about the relationships between these factors are fleshed out. In Section 3 the methods that have been used to answer the research question are explained, the used measures are clarified and the study design is discussed. In Section 4 the background and demographics of participants are given and the results are presented. In Section 5 first the implications of the results are discussed in light of the literature which was reviewed. Then some limitations of the study are considered and recommendations for future research are made. Finally concluding remarks will be presented in Section 6. Appended to this paper are additional information about the methodology, and additional statistical results.

2 Literature Review of Relevant Factors

In this section literature from the fields of cognitive and behavioural psychology, in particular on online privacy decision-making and economic trade-offs, will be discussed to get a grasp on how online privacy trade-offs work in terms of what psychological aspects can predict certain behavioural outcomes of trade-offs. The concepts which are generally thought to make up the main parts of privacy trade-offs are discussed. Also the factors that influence these main concepts, through heuristics and/or rational thought, are discussed. This discussion is loosely ordered from highest to lower relevance for this study. Additionally, based on the discussed concepts the hypotheses for this research are formed. See Figure 2 and Table 1 for an overview of the formed hypotheses.

2.1 Trade-offs

Acquisti et al. (2017) note that online trade-offs involving privacy are often rather complex for basically two reasons. Firstly, because of rapid developments in technologies and threats it is impossible for technology users to know what privacy threats they will be facing when agreeing to a certain choice. In addition, it is often unclear what information is collected, how this data is used and which parties are involved exactly. The GDPR combats this situation of ‘asymmetric information’ (meaning the consumer has less information about a trade-off than other parties involved) by giving users some legal rights to gain insight into these practices.

Secondly, there are cognitive processes that play a role in any trade-off, but can weigh in more heavily on trade-offs involving privacy (Acquisti et al., 2017; Acquisti, Brandimarte, & Loewenstein, 2015). First of all users have limited cognitive resources available to assess all possible outcomes of different choices. Making the rational approach of trade-offs involving privacy even harder is that privacy is usually not part of the main goal that users want to achieve when going to decide whether or not to use an online service. Spending cognitive resources on that part of the trade-off does not have priority. Besides cognitive resources people often have limited time to make a decision and don’t want to spend a lot of time on thinking through a part of the trade-off which is not about the main goal that they want to achieve by making the decision (Acquisti et al., 2017; 2015). Imagine the choice to be able to send pictures to friends when installing an app and therewith also agreeing to collection of sensitive information. The focus will probably be on being able to send pictures, because that is why the user came to visit the app store. The information collection has nothing to do with this goal and therefore invites less thought. Also, these unrelated domains can come across to people as contradictory and thus cause cognitive dissonance, which is then a feeling of mental discomfort about two seemingly incompatible domains (Festinger, 1957; Dinev, Xu, Smith, & Hart, 2013).

Apart from the cognitive functions, which make deliberate behavioural control possible, people rely much on mental short-cuts called 'heuristics' when making decisions in daily interactions with their environment (Gigerenzer & Goldstein, 1996; Gigerenzer, Todd, & the ABC Research Group, 1999). These heuristics are likely to have evolved in humans because decisions in daily life have to be made under conditions of limited knowledge of a situation, limited time and limited cognitive resources. This model of decision-making is generally called 'bounded rationality', as the ability to be rational is bounded by the aforementioned conditions and the environment (Simon 1956; 1982; Gigerenzer, 2004).

Heuristics are usually helpful, as they make it a lot easier to get through the daily choices. A different theoretical and methodological approach to model heuristics within the bounded rationality framework is the view that the behavior-steering nature of heuristics should be measured and that the effect it has on 'correct' behaviour should be called a 'bias' in behaviour or a 'cognitive illusion'. A bias is taken to be a certain behavioural tendency which makes behaviour consistently divergent from behaviour that is more correct from a purely rational point of view (Kahneman, Slovic, & Tversky, 1982; Camerer, 1998). Sometimes, probably in odd environments or situations, these biases can lead to the wrong choices by either letting people under- or overestimate certain risks and thus cause bad performance in that specific situation (Gigerenzer, 2004; Acquisti et al., 2017; Kahneman, Tversky, 1996).

When cognitive resources are taxed people have been found to be more likely to act on their impulses, falling back on the use of their heuristics more heavily instead of using rational calculation (Diamond, 2013; Veltri & Ivchenko, 2017; Kahneman & Egan, 2011; Mani et al., 2013a; 2013b). What makes privacy choices even more reliant on heuristics than other decision-making situations is that privacy risks often lie in the distant future, they are at the very least uncertain and are often also small in both their severity and their likelihood (Acquisti et al., 2017; Herley, 2009).

The takeaway is that privacy choices are often for a large part not purely rational. Trade-offs involving privacy are based on perception, bounded by cognitive resources and the environment and make use of heuristics which can result in behavioural biases. Even if someone would try their best to calculate all outcomes of possible decisions in a digital environment rationally, which they won't under usual time constraints, then the risks and benefits that someone can perceive of often do not present the actual risks and benefits because of lacking information and a rapidly changing environment. And while the benefits often seem clear and imminent (e.g. the prospect of immediately being able to use an app to send pictures to friends and the social benefits which that might bring), the risks (e.g. information disclosure or security breach to parties who might misuse the personal information (Dinev et al., 2013)) are highly uncertain, unclear and do often lie in the future. Additionally, it is usually the case that some private information has to be disclosed in order to receive benefits in some totally unrelated domain. As such, cognitive dissonance seems to be an element often occurring in privacy choices (Dinev et al., 2013).

From the above discussion of the psychological aspects of privacy trade-offs it becomes clear that people dealing with privacy trade-offs and have a high risk perception in those situations are prone to feelings of uncertainty, discomfort, cognitive dissonance (Dinev et al., 2013; Dowling & Staelin, 1994). Privacy concerns or high privacy risk perception triggered by specific situations, or more ever-present privacy concerns, seem likely to be able to cause diminished cognitive bandwidth, like monetary concerns have been found doing (Mani et al., 2013a; 2013b; Shafir & Mullainathan, 2013; Shah et al., 2012; Dean et al., 2017; Banerjee & Mullainathan, 2008). Several studies on economic trade-offs conducted by Mani et al. (2013a; 2013b) have yielded interesting insights into how concerns during decision-making could cause cognitive scarcity.

One of their studies in particular provided support for the hypothesis that trade-offs could cause cognitive scarcity and is particularly interesting to take note of in this context. In that study, Mani et al. (2013a; 2013b) gave different people four economic decision-making scenarios to think about, in between reading each scenario and answering what they would do if they were in the hypothetical situation, participants would be subjected to tests measuring their fluid intelligence and inhibitory control, which are both scientific constructs to grasp different parts of cognitive function. Two types of scenarios were used, one type per subject: financially easy (relatively cheap) scenarios or financially hard (expensive) scenarios. The hard scenarios were harder in that they were about how to come up with a larger amount of money to solve some hypothetical but realistic problem compared to the easy scenarios. The performance on the cognitive tests by the richer half of test subjects were unaffected by getting either financially easy or hard scenarios. The cognitive performance of the poorer half of subjects were significantly lower in the hard financial scenarios compared to the easy scenarios. This lead the authors to think that the hard scenarios triggered more financial concerns and distractions in the minds of relatively 'poor' people. Their interpretation was that financial concerns and distractions affected their cognitive abilities creating cognitive scarcity. Mani et al. (2013a; 2013b) studied economic trade-offs, but as stated before, the effects of monetary concerns could also be imagined to be applicable to concerns about risks in privacy trade-offs.

2.2 Inhibitory Control

Inhibitory control is a construct which is believed to be a measurable process of cognitive function. In their literature review on mental processes affecting economic decision-making, Dean et al. (2017) propose four categories of cognitive function that are interesting to study in relation to economic decision-making: attention, inhibitory control, memory and higher cognitive processes. Attention might be a factor that could influence online privacy decisions. For example, flashing advertisements may distract from important decisions about privacy. Also, in economic context Mani et al. (2013a; 2013b) have shown that significant effects of economic decision-making on fluid intelligence and inhibitory control exist for less wealthy people.

Fluid intelligence is one of two types of intelligence, which is a higher-order cognitive function. Fluid intelligence exists independently of previously acquired knowledge or skills and is often associated with memory processes, especially working memory (Dean et al., 2017, p. 18). While the higher-order cognitive functions of cognitive flexibility, intelligence and planning may all affect and be affected by decision-making in the context of online information disclosure, they are composed of several highly correlated lower cognitive functions and most of them fall outside of the scope of this research.

In their research on the influence of cognitive scarcity on online privacy disclosure, Veltri and Ivchenko (2017) review the literature of what causes people to rely more on their heuristics instead of conscious thinking in online privacy contexts. They point to two mental processes that, according to them, are affected most in the context of online privacy decisions, and that subsequently make people more likely to act on their impulses. The first mental resource they discuss is working memory, which is used to think reflectively. Working memory is specifically used to temporarily store and and manipulate information (Dean et al., 2017). It has been found that when working memory is being burdened by cognitive load, time pressure or other distractions it becomes harder to think reflectively (Veltri & Ivchenko, 2017). Thinking reflectively is highly necessary in privacy decisions, because they involve challenges such as balancing long-term comfort (e.g. not receiving annoying marketing emails) with short-term comfort (e.g. reading the annoyingly small print near the tick box or not).

The second mental process that can be affected according to Veltri & Ivchenko (2017) is ‘self-regulation’, the ability to restrain oneself from making impulsive decisions. It has been found that the ability to self-regulate is diminished after previous use of self-regulation. Since self-regulation supposedly draws from a limited supply it can actually be drained to cause ‘ego-depletion’ (Baumeister et al., 1998; Baumeister et al., 2007; Baumeister & Heatherton, 1996). The self-regulatory ability has been also called ‘cognitive control’ and ‘inhibitory control’ (Mani et al 2013a; 2013b; Dean et al. 2017), terms that stress that the ability is about inhibiting or restraining oneself from acting impulsively. This is important in privacy decision-making because to limit information disclosure people often need to restrain themselves from making the impulsively obvious and easy choice (e.g. just pressing the big green button saying ‘accept cookies’ instead of the small grey button to go into cookie settings).

Veltri and Ivchenko (2017) conclude from their research that both induced cognitive load on working memory and the straining of self-regulation make people significantly more likely to disclose more information online. They even found that working-memory load seemed to result in a little more information disclosure compared to ego depletion, but with only minor difference. Unfortunately, the model of inhibitory control as a limited resource has apparently not held under further scientific scrutiny. However, it is likely that situational factors do in fact influence inhibitory control, such as stress about risk beliefs and distractions in the environment (Dean et al. 2017). Nevertheless, inhibitory control remains a valid concept to try to explain choice behaviours.

The most clearly overlapping measure that is used in both the study by Mani et al. (2013a) and the study by Veltri and Ivchenko (2017) is inhibitory control. Thus to study cognitive bandwidth in this study inhibitory control will be measured for use as a dependent variable to research the relationship between privacy decision-making and cognitive function.

Predictors of Inhibitory Control. Since situational monetary concern was found to limit cognitive function, it seems likely that in a privacy context some kind of situational privacy concern should have the same role. The goal of this research is to investigate the effect of the worry about privacy risk in a given situation. The two following predictors from the literature about privacy trade-offs are worth considering here. But only one of them, ‘risk belief’, is hypothesized to have the highest potential to affect inhibitory control in this research.

Pre-Existing General Privacy Concern. One predictor of inhibitory control could be pre-existing general privacy concerns. These pre-existing concerns might be a source of distracting thoughts and stress which are formed during a privacy related decision-making process (Dinev et al. 2013). General privacy concerns are believed to be pre-existing or dormant until activated (Kehr, Wentzel, Kowatsch, & Fleisch, 2015; Buchanan, Paine, Joinson, & Reips, 2007; Marreiros, Tonin, Vlassopoulos, & Schraefel, 2017). These concerns have been found to negatively affect perceived risks and affect stated behavioural intention directly (Kehr et al., 2015; Malhotra, Kim, & Agarwal, 2004). However, they are not dependent on the context of any particular privacy trade-off.

Risk Belief. Risk belief is a core privacy construct mostly believed to influence behavioural intention together with perceived benefits (Kokolakis, 2017; Kehr et al., 2015). Risk belief is the risk that is perceived in the situation of the privacy trade-off, and is both affected by pre-existing general privacy concerns and by other contextual factors. Here risk belief is explained in view of that it may influence inhibitory control. In research on economic trade-offs is has been theorized that relative or experienced poverty and not absolute poverty causes financial worries during economic trade-offs (Mani et al., 2013). It is the experienced gap between monetary possession and need which is a measure of this relative poverty. In the context of privacy, the immediate concerns about the gap between the privacy situation before disclosing information and the level of privacy that a person would like, would be measured better by situational risk belief than by pre-existing general privacy concerns. Thus risk belief will be taken into account as a predictor for inhibitory control, leading to the following hypothesis:

H1a: Risk belief negatively affects inhibitory control.

Protection Belief. It has been suggested that the belief about protection measures should be part of measuring overall privacy concern (Buchanan et al., 2007). A closely related construct of 'information control' was found to have a positive effect on a separate construct called 'perceived privacy' (Dinev et al., 2013). Additionally it could be hypothesized that perceived protection sufficiency might also affect inhibitory control directly. When a personal protection level is believed to be insufficient to control personal information, then that might be a cause of worry. Therefore, the perceived level of protection against privacy violation will be included as a predictor of inhibitory control in this study. To that end the following is hypothesized:

H1b: Protection belief positively affects inhibitory control.

2.3 Risk Belief

Contrary to the previous section where risk belief was dealt with in its role of potentially influencing inhibitory control, in this section risk belief is treated as a dependent variable. Risk belief is the factor of the privacy calculus that is cited in most models as affecting behavioural intention. Apart from being called 'risk belief' (Malhotra et al., 2004) it also goes under the name of 'expected loss' (Kokolakis, 2017) or 'perceived risk' of information disclosure (Kehr et al., 2015; Dinev et al., 2013), which are basically different names for the same construct. It was already mentioned in the previous section that the perceived risks and perceived benefits are weighed by the decision maker to form a decision. When keeping the benefits of a certain trade-off of similar value to all participants in this study, measuring risk belief would be sufficient to see if there is an effect in any cognitive functions. Any negative affect which would affect risk belief as Kehr et al. (2015) measure, would not matter when the main point of interest is the influence of risk belief on the variables such as inhibitory control, behavioural intention and willingness to pay.

Predictors of Risk Belief. First of all it is important to note that privacy decisions are highly contextual, and that it varies per situation and environmental factors how people perceive risks and benefits (Kokolakis, 2017; Veltri & Ivchenko, 2017; Kehr et al., 2015). It seems from the discussed literature that the perceived risks of information disclosure within a privacy situation capture both to a large extent general privacy concerns (Kehr et al., 2015; Malhotra et al., 2004), *and* the actual contextual factors of the situation, such as the sensitivity of the information that is to be disclosed (Dinev et al., 2013; Malhotra et al., 2004), the perceived benefits, and pre-existing moods (Kehr et al., 2015).

Pre-Existing Affect. A pre-existing happy mood was found to mainly reduce risk perception and pre-existing sadness tempering that effect (Kehr et al., 2015). In addition, Veltri and Ivchenko (2017) found that valence and the emotion of anger negatively impacted actual online information disclosure behaviour, mostly when working memory had been stressed. Because mood or affect is supposed to be captured well in risk belief and behavioural intention, the affect is not going to be a part of this study. Also, the inclusion of mood tests might complicate and lengthen the survey too much for the value it adds to this research project.

Information Sensitivity. One of the important situational factors that have been found to increase the perceived risk is the sensitivity of the disclosed information (Kehr et al., 2015; Dinev et al., 2013; Malhotra et al., 2004). It seems to be the most influential factor that controls risk belief. Because information sensitivity is very important and easy to manipulate a study using (hypothetical) privacy scenarios, it will be included in this study as a treatment variable with two conditions. The hypothesis accompanying information sensitivity is:

H2a: Information sensitivity positively affects risk belief.

Protection Belief. As stated earlier in Section 2.1 it has been suggested that the belief about protection measures should be part of measuring overall privacy concern (Buchanan et al., 2007). Additionally, a closely related construct of 'information control' was found to have a positive effect on a separate construct called 'perceived privacy', but in that study its relation to risk belief directly was not tested (Dinev et al., 2013). Moreover, it seems logical that the belief about having sufficient measures in place or not, affects the belief of the situational risk. For example, if someone believes to generally have taken enough protection measures (e.g. having a good spam filter or using an email alias) this person might have a lower risk belief (e.g. when the trade-off is about online disclosure of their email address). The hypothesized relationship between protection belief and risk belief is the following:

H2b: Protection belief negatively affects risk belief.

Experienced Privacy Violations. While is seems that the frequency that someone had their own privacy violated would have a positive effect on risk belief, previous research has not been able to find any significant effect of experienced privacy violation on risk belief (Malhotra et al., 2004). In this previous study only a quite general risk belief was asked of the participants (about privacy trade-offs in online commerce in general). It would be interesting to see if the effect is significant if the risk belief is measured for a specific scenario. That is the aim of the current study. The hypothesized effect of experienced privacy violations is the following:

H2c: Experienced privacy violations positively affect risk belief.

Exposure to Messaging about Privacy Vulnerabilities. Previous research found that a high frequency of exposure to media about information misuse resulted in a higher value of a construct called 'trusting beliefs'. Trusting beliefs was hypothesized and shown to be able to negatively affect risk beliefs (Malhotra et al., 2004). One could think of why this kind of exposure would lead to higher risk belief, by or apart from influencing a belief of trust in companies handling peoples' data. A plausible explanation is that the perception of the risk gets higher because the media content feeds the 'availability bias' (Acquisti et al., 2017). The availability bias means that a risk perception is pumped up (e.g. the risk of supplying your credit card number to an online shop), because when thinking about a certain trade-off what comes to mind first are all those messages that make the risk seem high (e.g. a lot of messages about massive credit card number thefts). These messages make the information about large risks very available in the mind. Thus, the direct relationship between exposure to messaging about privacy vulnerabilities and risk belief is hypothesized as follows:

H2d: Exposure to messaging about privacy vulnerabilities positively affects risk belief.

Education. Education was found by Malhotra et al., (2004) to negatively affect the construct of trusting beliefs. Since they also saw that trusting beliefs were negatively affecting risk belief, it seems like education could have a positive direct effect on risk belief as well. Another study found that higher education significantly lowered the amount of actual information disclosure (Veltri & Ivchenko, 2017). This could also have been because education had positively affected risk belief. Education can indeed cause lower trust generally because a higher education level might have trained people to look more critically upon the world. But also more general awareness of privacy risk because of the critical worldview or related media exposure might be the cause of the effect of education on risk belief. It would be interesting to find that this hypothesized relationship could be supported by this research:

H2e: Education positively affects risk belief.

Age. Age was found to be negatively related to behavioural intention (Malhotra et al., 2013). Since risk belief seems to be a reliable predictor for behavioural intention, one could wonder what the effect of age on risk belief would be. It should be noted hat probably age has a positive correlation with education, and education probably has a positive effect on risk belief. Therefore education should be considered as being a mediator in the relationship between age and risk belief.

H2f: Age positively affects risk belief.

2.4 Behavioural Intention

The behavioural outcome of a decision process is often not recorded directly in research, but captured in the concept of 'behavioural intention': what someone states that they would choose in a given situation. To measure the behavioural outcome of a trade-off it would be best to measure the behaviour instead of the behavioural intention, of course. However, this is not always practically feasible in research, because of either ethics considerations or technicalities. Moreover, peoples' behavioural intention is generally taken to quite accurately display their actual behaviour in the context of information disclosure and "within the framework of reasoned action" (Malhotra et al., 2004, p. 342).

Predictors of Behavioural Intention. The intention of people to disclose sensitive information in their actual behaviour are managed by a situational privacy calculus, which is a process which is highly dependent on the context of the trade-off. (Kokolakis, 2017; Kehr et al., 2015; Malhotra et al., 2004). This situational calculus consists mainly of deciding upon the expected loss of disclosure (the risk belief) and the expected gains (perceived benefits) of disclosure (Kokolakis, 2017; Kehr et al., 2015). In most of the research on this topic risk belief is a stable factor which is included in most models as a main predictor for behavioural intention, followed by perceived benefit (Kokolakis, 2017; Kehr et al., 2015; Malhotra et al., 2004).

Perceived Benefits. In previous research the construct of perceived benefits has been found to positively affect willingness to disclose private information (Kehr et al., 2015). It has also been found that the perceived benefits can have some negative effect on the level of the believed risks (Kehr et al., 2015; Dinev et al., 2013). Perceived benefit is the part of the decision-making process that can be expected to limit cognitive function less than risk belief. Therefore the focus will lie on risk belief in this study. The benefits can be kept relatively constant in order to focus on the impact of risk belief. It is therefore not necessary to include perceived benefits in this study.

Pre-Existing General Privacy Concerns. General privacy concerns were also found having a direct negative effect on behavioural intention (Kehr et al., 2015). The effect was of about half the size of the effect on risk belief. For brevity and because measuring situational risk beliefs and other situational factors is more important, general privacy concerns are not measured in this research.

Risk Belief. As risk beliefs are the predictor that is likely to induce uncertainty, discomfort or anxiety (Dinev et al., 2013), it is the predictor of behavioural intention which is expected to limit cognitive function the most. Therefore it is a main component of this study. Risk belief has been found to have a negative effect on behavioural intention (Kehr et al., 2015; Malhotra et al., 2004). In fact, risk belief has been found to have a negative effect on actual information disclosure behaviour in online social-networking situations as well (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). The hypothesized relationship between risk belief and behavioural intention is then the following:

H3a: Risk belief negatively affects behavioural intention.

Age. Age was found to be negatively related to behavioural intention (Malhotra et al., 2013). This effect will be tested in this study as well to provide a frame of reference to previous studies. Therefore it is hypothesized that:

H3b: Age negatively affects behavioural intention.

2.5 Willingness to Pay for Non-Disclosure

In the field of behavioural economics researchers have tried to measure the amounts that people are willing to pay (WTP) as an alternative way to measure behavioural intention (Acquisti, Taylor, & Wagman, 2016). But because of a myriad of reasons putting a simple price tag on privacy is problematic. One of those reasons is that there are benefits at play as well, not only risks. This and use of heuristics are some of the reasons why the 'privacy paradox' was also found in the monetary difference between what people are willing to pay to keep personal information to themselves and how much they are willing to accept in exchange for their information. However, it was shown that some people would pay a small premium of about of about 50 dollar cents for products costing $15 to buy them from a more privacy protective merchant (Tsai, Egelman, Cranor, & Acquisti, 2011). And in a separate study people were found to be willing to pay $1.75 to conceal their phone's identification number (Savage & Waldman, 2013). If benefit is kept equal then a willingness to pay for non-disclosure of personal formation might actually say something about the worth that is assigned to this information and the perceived risks within a given trade-off. It might closely related, and perhaps in some degree an alternative to, behavioural intention.

Predictors of Willingness to Pay. Willingness to pay is much related to behavioural intention. Opposite to behavioural intention which tells what choice a person is likely to make, WTP would betray the monetary worth that a person would give to avoid making a certain choice and keep the privacy status quo. There are some likely predictors of willingness to pay that will be included in this study.

Risk Belief. Risk belief might have an effect on willingness to pay similar to the effect of risk belief on behavioural intention. It is likely that the higher the risk belief is the more someone would be willing to pay to avoid that risk. Perceived benefits have to be kept as constant as is possible of course. The relation between risk belief and WTP is hypothesized as follows:

H4a: Risk belief positively affects willingness to pay for non-disclosure.

Age. As age was found to be negatively related to behavioural intention (Malhotra et al., 2013), it is likely that age would also be positively related to WTP. This effect should be controlled for rising income (by age) to see if then there still is a meaningful effect left. The hypothesis is therefore:

H4b: Age positively affects willingness to pay.

Protection Belief. In addition to risk belief affecting WTP, someone with a perceived level of protection that would not be sufficient to prevent privacy harms, might pay more to avoid information disclosure. Thus protection belief could have a negative effect on WTP. The following hypothesis should be tested:

H4c: Protection belief negatively affects willingness to pay.

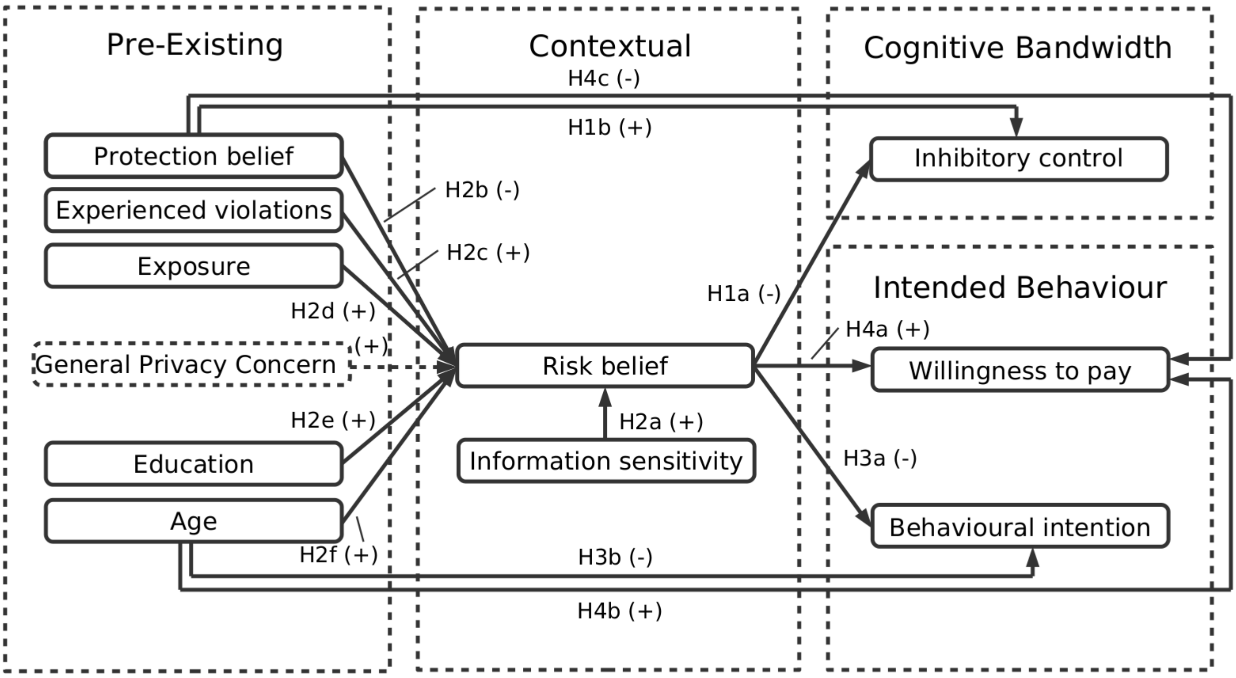

Fig. 2. Model showing the hypothesized relations that are explored in this study. 'General privacy concern' is shown for more complete understanding, but is not measured in this study.

Table 1. Hypotheses of interest in the order in which they were presented.

Number	Dependent Variable/Hypotheses
1	**Inhibitory Control**
a	Risk belief negatively affects inhibitory control.
b	Protection belief positively affects inhibitory control.
2	**Risk Belief**
a	Information sensitivity positively affects risk belief.
b	Protection belief negatively affects risk belief.
c	Experiences of privacy violation positively affects risk belief.
d	Exposure to messaging about privacy vulnerabilities positively affects risk belief.
e	Education positively affects risk belief.
f	Age positively affects risk belief.
3	**Behavioural Intention**
a	Risk belief negatively affects behavioural intention.
b	Age negatively affects behavioural intention.
4	**Willingess to Pay (WTP)**
a	Risk belief positively affects willingness to pay for non-disclosure.
b	Age positively affects willingness to pay for non-disclosure.
c	Protection belief negatively affects willingness to pay for non-disclosure.

3 Methodology

3.1 Survey Administration, Study Design and Measures

To test the hypotheses that were formed in the previous section the approach was taken to use an online survey and an online cognition test which was more or less embedded into the survey. The paragraphs below describe what was presented to the participants, which had the same order in which it is explained here.[1] The survey was divided into several pages, containing instructions, a scenario, a group of questions per page, or just one question per page. The survey was distributed to the first participants on the night of Friday 25 May 2018, which interestingly was the day on which the GDPR derived law had gone into effect in The Netherlands and had gotten a lot of media attention. The survey stayed open for participation for 10 days, but was only actively promoted by the author for 8 of those days. Most participants had made the test during the opening weekend and the Monday directly following that weekend.

Recruitment of Participants and Start of the Survey. The participants for this survey were recruited in three ways: a digital privacy advocacy organisation called 'Bits of Freedom' would post a link to the survey on their Twitter account, the survey was administered to a final year bachelor class consisting of humanities students from a myriad of different studies, and people from the personal network of the author (mostly relatives, friends, Media Technology classmates, and ex-colleagues within a slightly activist or technical scene) would be asked mostly by means of personal messages or social media posts to partake in the study. All participants were made aware of the fact that a restaurant gift card worth 30 euros could be won if they participated. All participants would receive the same link to the landing page with general information about the study and about the data collection practices. From there they followed a link to the online survey where they were presented with more detailed information about the study and had to consent and state to be at least 18 years of age to continue. It was also strongly advised to use a touchscreen device to partake in the study.

Referral or Segment and Screen Type. The Thereafter two questions were asked. One was about in which way they were lead to the survey ("How did you reach this survey?") for which the answers were "In connection to Bits of Freedom", "It was conducted with me in class or at school/university" or "Other". This question was included to be able to tell apart post hoc roughly to which group the participants belonged. This might be important as people which were

[1] Copies of the full survey and of the Simon task that were used in this study may be requested from the author.

connected to Bits of Freedom in particular might have a much higher dose of media exposure on the subject of privacy vulnerabilities than the others, and perhaps a higher risk belief in general.

The other question was if they were using a touchscreen device or a non-touchscreen device to partake in the study. This distinction was made because the cognition test or ‘Simon task’ was made to be most effective and precise in measuring inhibitory control for touchscreen users. If the participant reported using a touchscreen for the survey, then they were asked to put their smartphone into ‘Do Not Disturb’ mode before continuing if they were using a smartphone, to avoid notifications interrupting the survey and test.

Demographics. First some demographics questions were asked, which could be used as control variables during analyses. Nationality could be selected from a drop down list of countries. Participants were asked what their gender was (“Male” or “Female”). They were asked about their age using 6 bins of roughly 10 years per bin (“18-24”, “25-34”, “45-54”, “55-64” or “65+”). Participants were asked about the highest level of education that they had obtained a degree from (“High school VMBO”, “High school HAVO”, “High school VWO/Gymnasium”, “MBO”, “HBO (university of applied sciences)”, “WO Bachelor (university)”, “WO Master (university)”, “PhD”, or “Other:” with this last option having a field to state their level of education). Then they were asked what best described their current occupation (“Student, full-time”, “Student, part-time”, “Working, as a paid employee”, “Working, self-employed”, “Not working, on temporary layoff from a job”, “Not working, looking for work”, “Not working, retired”, “Not working, disabled” or “Not working, other”). Finally they were asked about their monthly income after tax deduction, and given instruction to “Please include any income from a student loan and other sources of income (e.g. contribution by parents, regular monetary investment returns)”. This question was mostly divided into 10 bins of 500 euros, an answer for anything above that, and the option was given not to answer (“€ 0 – 500”, “€ 500 – 1.000”, “€ 1.000 – 1.500”, “€ 1.500 – 2.000”, “€ 2.000 – 2.500”, “€ 2.500 – 3.000”, “€ 3.000 -3.500”, “€ 3.500 – 4.000”, “€ 4.000 – 4.500”, “€ 4.500 – 5.000”, “more than € 5.000” or “I prefer not to answer”). The “I prefer not to answer” option would be considered a missing value during most post hoc analysis.

Privacy Trade-off Scenario. Then participants were randomly divided into either of two conditions. After which they were presented with a hypothetical online privacy trade-off scenario that differed per treatment in the kinds and amount of sensitive information that it was about. Participants were asked to “Please take a moment to think about what you would do in the following scenario:” The two scenario’s where as follows:

Low Information Sensitivity Scenario. One of these scenarios was about only gender and age:

> *You are visiting the website of a discount club called 'FreeLy'. The club offers a discount to consumer products, venues and events (e.g. electronics, museums, hotels, festivals) to its members.* ***Imagine, you are interested in joining.*** *To make an account your email address is required. Next, there are two membership options:*
>
> <u>*Paid*</u> *- You pay an annual membership fee of €20 and have to provide no further information.*
>
> <u>*Free*</u> *- For this option you are required to fill out your gender and age (DETAILS). You have to update this information annually.*

High Information Sensitivity Scenario. In the other scenario the information that had to be disclosed was their telephone number, house address, nationality and your personal occupational and financial information:

> *You are visiting the website of a discount club called 'FreeLy'. The club offers a discount to consumer products, venues and events (e.g. electronics, museums, hotels, festivals) to its members.* ***Imagine, you are interested in joining.*** *To make an account your email address is required. Next, there are two membership options:*
>
> <u>*Paid*</u> *- You pay an annual membership fee of €20 and have to provide no further information.*
>
> <u>*Free*</u> *- For this option you are required to fill out your telephone number, house address, nationality and your personal occupational and financial information (DETAILS). You have to update this information annually.*

These two scenario's where adapted from Malhotra et al., (2013). For this research they were changed to include a hypothetical company called 'FreeLy' to make them applicable to one specific situation. Also they included information that the participants had just entered themselves on the previous demographics page of the survey to make the scenario feel more real or imminent. These details where listed on the position of the *DETAILS* placeholder in the scenario's cited above. In the high information sensitivity condition it would for example say "(Netherlands, Female, 25-34 years old, WO Bachelor (university), Working, as a paid employee and an income of € 2.000 – 2.500)". If income had not been provided than the *DETAILS* would just end in "… and your income)".

The upside of using these scenarios is expected to be that the perceived benefits from the privacy calculus are kept relatively constant across different participants. This is done by specifying a specific amount for the member fee. Moreover, by including a wide range of benefit domains ("consumer products, venues and events (e.g. electronics, museums, hotels, festivals)") users are encouraged to pick in their minds what they would be most interested in. The scenario also leaves room for personal expectations about benefit. By means of the combination of "discount" and given that the participant is "interested in joining" they can imagine themselves for what level of discount they would start to be interested in joining were this a scenario in real life. While this benefit is then relative per person, it is relatively the same benefit: it is the discount threshold to which they would join such a program. The relative level of perceived benefits is in this way kept similar for every participant.

Risk Belief. Thereafter participants were presented with five statements targeted at the scenario which were measuring risk belief. The specific informational items that were included in the scenario were also included in these statements. For brevity only the statements from the low information sensitivity condition are given here as an example. The statements of the high information sensitivity condition are exactly the same but for the stated personal information. The participants needed to rate the level to which they agreed to the statements on a 7-point Likert-type scale, choosing between "Strongly disagree", "Disagree", "Somewhat disagree", "Neither agree nor disagree", "Somewhat agree", "Agree" or "Strongly agree". The statements were adapted from the five statements used by Malhotra et al., (2004) to measure the construct of risk belief as part of their Internet User Information Privacy Concerns (IUIPC) scale, and changed to target the specific scenario in this study. The five statements in the condition of low information sensitivity were:

> *I would find it risky to give my gender and age to FreeLy.*
>
> *There would be a high potential of personal damage associated with giving my gender and age to FreeLy.*
>
> *There would be too much uncertainty for me associated with giving my gender and age to FreeLy.*
>
> *Providing FreeLy with my gender and age would involve many unexpected problems.*
>
> *I would feel safe giving my gender and age to FreeLy.*

The statements used by Malhotra et al., (2004) and a selection of them later by others (Dinev et al., 2013; Kehr et al., 2015) have been a tried way to be able to measure risk belief for the general context of information disclosure in online commerce or online interactions. For the purpose of this study these five questions have been altered to be situational; to be specifically about the situation in the scenario which is presented to the participant. From a Principal Component Analysis (PCA) on the answers to the five statements/questions used in this study, it was concluded that all five questions are quite equally loaded and the principal factor performs as well as taking the average of the five questions. The five questions were therefore averaged to form the variable 'risk belief'.

Behavioural Intention. Then the participants would be asked about the extent to which they would actually reveal the information given their scenario. Two statements were presented to this end. The information content of the statements presented here is that of the low information sensitivity condition as an example. The high information sensitivity condition featured the same two statements but then including the information of that scenario instead. One statement in the low information sensitivity condition was "How likely would it be that you would reveal your gender and age to FreeLy, given that this saves you €20 per year?", which had to be rated by participants on a 7-point Likert-type scale with the options: "Very unlikely", "Unlikely", "Somewhat unlikely", "Neither likely nor unlikely", "Somewhat Likely", "Likely" and "Very Likely". The other statement in the low information sensitivity condition was "How willing would you be to reveal your gender and age to FreeLy?”, to which participants had to select one of the following options on a 7-point Likert-type scale: “Very unwilling”, “Unwilling”, “Somewhat unwilling”, “Neither willing nor unwilling”, “Somewhat willing”, “Willing” and “Very willing”.

To measure the intention to exert disclosure behaviour, the two statements explained above were adapted from two of the four questions used by Malhotra et al., (2004) to measure ‘behavioural intention’. They were changed to refer to the specific scenarios of this research. The two other statements which were used by Malhotra et al., (2004) were about the probability and possibility of disclosing information. They were considered respectively to be a duplicate to one of the other questions and unclear in their meaning when applied to the specific scenario for this study.

Inhibitory Control. Thereafter the participants were linked to an online cognitive test (specifically a ‘Simon task’) which was stated to the user to measure their “reaction time”. A product of the Simon task is a measurement termed the ‘Simon effect’ which is a measure of inhibitory control (Dean et al., 2017). The Simon task was conducted on the online PsyToolkit platform. An adaptation of the readily available Simon task demo on PsyToolkit was used (Stoet, 2017; 2010). It was optimised for use of a touchscreen. The test started with a few instruction screens. The participant was presented with the following instructions. Two circles were to be shown side by side. Always one of the circles was white and the other one red or green. The participant always had to press the left circle when one of the circles was red, no matter which of the two circles was red. If one of the circles was green then the participant always had to press the right circle, no matter which of the two circles was green. Participants were asked to be as fast as possible while still being accurate. This set of rules resulted in basically two conditions: either the circle that was colored was the circle that has to be pressed, or the the colored circle was opposite to the circle that needs to be pressed. These conditions are called ‘congruent’ and ‘incongruent’ respectively.

Then four trials were given to the participant as practice trials. After which once more one of the instruction screens was presented giving a recap of the rule. Thereafter 36 real trials were administered to the participant. Then a pause screen was presented, giving the participants a brief moment to catch their breath and to muster new focus to complete the next trials. Also the congruent and incongruent reaction times in milliseconds were given on this screen (disguised as “Time A” and “Time B”) to give the participants some feedback and motivating them to keep performing in the second round. When the participant felt ready they would continue to the next 36 trials. When the end of the test was reached participants were instructed to copy a token and return to the survey using a link. There they had to paste their unique test token in a field in the survey. This token would be used to connect the data collected by the cognitive test platform to the survey responses of the same individual post hoc.

The time between trials was 500 milliseconds. After a wrong circle was pressed, there was pressed outside of the circle or time out had been reached after 5000 milliseconds, then an error screen would be shown for 1200 milliseconds (2600 if during the four training trials). Trials where randomly selected from the four possible conditions: green congruent, green incongruent, red congruent and red incongruent. See Figure 3 for a few of the screens that were mentioned in the above explanation.

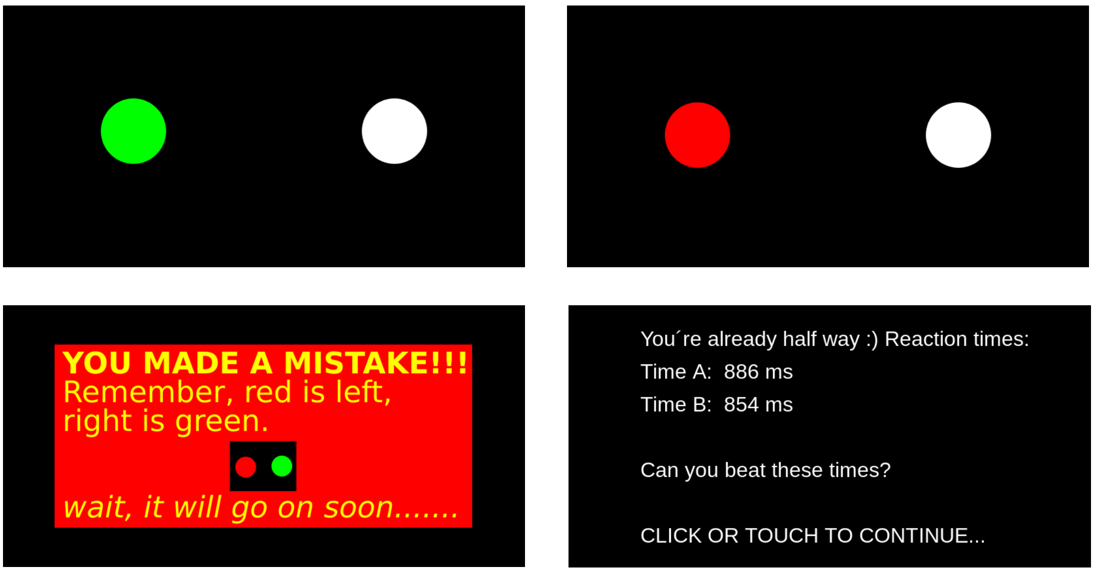

Fig. 3. Screenshots of different stages of the Simon test. An incongruent green condition (upper left). A congruent red condition (upper right). A mistake screen (bottom left). Pause screen halfway during the test (lower right).

To understand how the Simon task measures inhibitory control some theoretical background is in order. The average time spent longer on incongruent trials versus congruent trials (incongruent - congruent) is called the 'Simon effect' and measures inhibitory control (Dean et al., 2017). People are generally a little faster in congruent conditions than in incongruent conditions. In their review of measurement techniques for inhibitory control, Dean et al., (2017) list the Hearts and Flowers task, Eriksen Flanker task, and Stroop task as the most prominent ways to measure inhibitory control. They note that the Stroop task has been criticized for not accurately measuring inhibitory control. The Hearts and Flowers task has been criticized for also involving working memory due to remembering two different figures. The Simon task, an older similar task, does not suffer from this complication because it shows very similar stimuli and only uses one simple game rule. Because of the theoretical advantages and its ease of distribution online the Simon task was chosen to measure inhibitory control.

Willingness to Pay. The participants were then asked for their willingness to pay to avoid sharing the information of their scenario. The question for the low information sensitivity condition was "Imagine that you are determined in joining discount club 'FreeLy'. What is the maximum annual amount you would be willing to pay to avoid sharing your gender and age? (in whole euros)". The participant could enter any amount between and including 0 and 999 euros. But this range was only given back in the form of an error after the participant had entered something that was not a number in this range, to avoid anchoring these numbers in the participants mind to begin with (Acquisti et al., 2017).

Expectations of Violation, Past Violations and Media Exposure on Information Misuse. Then the participants were asked to answer some questions about their expectations and experiences. First three questions were presented on one page. The expectation of the frequency of falling victim to privacy violations in the future was supposedly measured by the question "In the future, how frequently do you expect to personally be the victim of an improper invasion of your privacy?" The frequency of having ones privacy violated in the past was measured using the question "How frequently have you personally been the victim of what you felt was an improper invasion of your privacy?" Exposure to messaging about privacy vulnerabilities (specifically misuse of information collected on the internet) was measured using the question "How frequently have you heard or read during the last year about the use and potential misuse of the information collected on the Internet?" All three of these questions had to be answered on the following 7-point Likert-type scale: "Very infrequently", "infrequently", "Somewhat infrequently", "Neither frequently nor infrequently", "Somewhat frequently", "Frequently" and "Very frequently". The questions about exposure to messaging about privacy vulnerabilities and experienced past violation have been adapted from Malhotra et al., (2004) and only their 7-point scales were changed, mostly to be more clear and complete instead of just giving the two extremes and letting the user decide the meaning of the points in between.

Protection Belief. Thereafter participants were asked to consider to what extent the following statement applied to them: "I believe that in general I have taken enough precautions to protect me from improper invasion of my privacy." Which they had to answer on a 7-point Likert-type scale by choosing between "Strongly disagree", "Disagree", "Somewhat disagree", "Neither agree nor disagree", "Somewhat agree", "Agree" or "Strongly agree". This question was used to try to measure the perceived sufficiency of the protection level by the participant. A perceived insufficient protection level might cause worries, which could influence the variables of risk belief, inhibitory control, behavioural intention and willingness to pay.

Survey End. After that the protection belief was measured. Finally a field was given for participants to write their email address if they wanted to partake in winning a restaurant gift card worth 30 euros, stating that the alternative for filling in their email address in that field was sending an email to the principal investigator with the subject line "WINNING". Thereafter the participants were thanked for their time.

3.2 Approach to Statistical Analysis

The approach that has been taken in the statistical analyses of the data needs explanation on two subjects: the meaning of significance and the approach to providing evidence for mediation.

Practical and Statistical Significance. An important note needs to be made to most of the research on modeling privacy trade-offs discussed in section 2. The fact that in many of them the statistical significance (the value of p) takes precedence over the 'real world significance' effect size in combination with an actual error measure in the form of a confidence interval in the interpretation of statistical results. However, only focusing on p-values and not reporting on the effect sizes that can be expected of parameters for a certain model is very limited in its real world significance and the p-value can be influenced by sheer sample size (Ziliak & McCloskey, 2008; 2004; Gill, 1999). Therefore, model variables in this study will mainly be interpreted by the size of their coefficients and their respective standard errors and confidence intervals. Their statistical significance will be an addition to this discussion more on the background. When only stating ‘significance’ in this paper this should be interpreted as at least the fact that the 95% confidence interval is bounded away from zero, meaning that the effect could not be either negative or positive but falls on one side of zero.

Mediation. To test if a variable is a mediator between two other variables the method originally developed by Baron & Kenny (1986) and deployed in a similar setting by Dinev et al., (2013) was used. Mediation can be useful to explain how the seemingly direct relationship between two variables (e.g. A → C) can be explained statistically by a mediatory relationship through a mediator variable (e.g. B as mediator variable, so A → B → C). In short, a variable, for example B, can be said to be a mediator between two other variables, for example A and C, when three conditions are met. Firstly, the relationship between A and B needs to be statistically significant. Although I would argue that instead of looking a the p-value the confidence interval is more useful and reliable. Secondly, the relationship between A and C needs to be significant. Finally, the effect of A on C needs to become weaker or less significant when the mediator variable B is included in the regression model, compared to when it is not included in the regression (Dinev et al., 2013).

4 Results

After the survey was closed, the data was cleaned as is described next. First the participant data of the Simon task were matched to the participant data of the survey by matching the unique codes per participant contained in both data sets. After that had been done, 131 participants seemed to have at least completed the study so far that they had entered their unique Simon task code in the survey. First, participants who did not finish the survey all the way to the end were excluded. Secondly the data belonging to a test run of the author was removed. Thereafter a country was added in exchange for another country for one of the participants who had contacted the author that their country had not been included as an option in the drop down. Additionally, based on analysis of the education data the decision was made to add the level of “Primary” school instead of “Other:”. This was acceptable because only one participant had chosen “Other:” with the comment that they had only officially finished primary school. Next, age, education and income were made into ordinal variables from low age, educational level and income to high.

Thereafter, only participants who used a touchscreen were included. The Simon task had been optimized for use of touchscreen. Using a mouse was possible but this would cause a lot of interference because the mouse had to be moved from one circle to another. This would measure more of the time to move the mouse than the time it took for the brain to decide to press one circle or the other (Sternberg, 2004). This was not the case for touchscreen users which could use two hands or one hand to move much faster to the buttons of choice. Then one participant was excluded who spent more that 10 minutes on the Simon task. This would not measure any effect anymore related to this study. The test would for the most participants not take longer than 6 minutes, and for many a couple of minutes shorter. Also participants who took over 40 minutes to finish the whole survey (including the Simon task) were excluded, which resulted in only one exclusion of a participant taking 110 minutes to complete the whole survey. This length would have a very high chance of resulting in data that did not measure the effects that were needed to be measured as reliably as possible.

Then the “I prefer not to answer” answers for income were replace by NA values so that the income values that were provided by other participants could be used as an ordinal variable. All answers to (7-point) Likert-type scale questions were ‘centered’ by subtracting the number 4. This way of centering was chosen instead of subtracting the mean, in order to keep the regression coefficients interpretable in terms of their original 7-point scales. Risk belief and behavioural intention were calculated by averaging the thereto belonging questions. Also the construct of Simon effect was computed by subtracting the mean congruent value from the mean incongruent value per participant.

In a Simon task, trials after erroneous trials tend to elicit a longer reaction time compared to trials following successful trials. It has therefore been practiced by researchers in the field of cognitive psychology to exclude the trials after erroneous trials for analysis in order to increase stability and accuracy (Sternberg, 2004). The Simon effect for this study was calculated on both data including trials after error trials and on data excluding trials after errors. The resulting different distributions of the Simon effect can be seen in Figure 4. Simon effects are mostly supposed to be positive because people are on average slower for incongruent trials than for congruent trials. It is therefore interesting to note that for the data set containing all correct trials still 27 participants (26%) had a Simon effect below zero, and for the data set excluding (so including only trials after successful trials) resulted in 28 participants (27%) with a Simon effect below zero. In addition, the median of the data set including only trials after successful trials was much lower than the data set that was derived from all correct trials. Also it can be seen that on the right tail of the distribution for the data set for only trials after successful trials, some irregularities spring up which make the data less normally distributed. For these reasons, the Simon effect based on the data set derived from including all correct trials was used in the further analysis of the results.

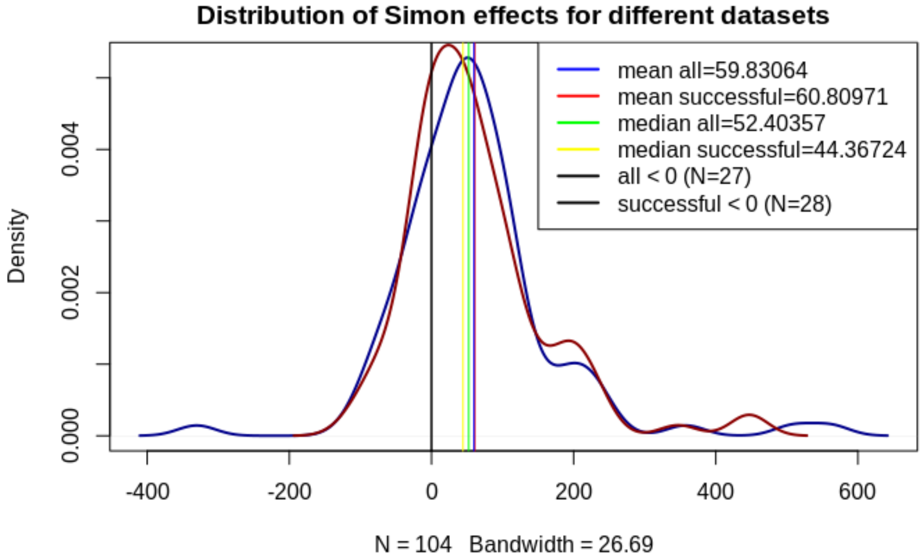

Fig. 4. Distributions of Simon effect for the data set only trials after successful trials are included (“successful”) and the data set in which all correct trials were included (“all”).

4.1 Description of Sample

Of the remaining 104 participants 53% reported being female and 47% male. 25% of participants had reached the survey in connection with Bits of Freedom, 22% said the survey was conducted with them at university and 53% provided “Other”. Of the provided education levels a university master degree was most common among participants with 36%, followed by high school VWO (21%), university bachelor (20%), university of applied sciences (17%) and the remaining 6% thinly spread over other levels. 36% of participants reported being between 18-24 years old, 33% between 25-34 years old, 13% between 35-44 years old, 10% was between 45-54 years old, 9% between 55-64, and 1% reported 65 or older. While 13% of participants did not report their income, the biggest group from those who did was at € 500 – 1.000 (28%), followed by € 1.000 – 1.500 (14%), € 2.000 – 2.500 (13%), € 1.500 – 2.000 (9%), € 2.500 – 3.000 (8%) and the remaining 15% spread across the other income bins. A total of 57 participants (55%) received the high information-sensitivity treatment and 47 participants (45%) the low information-sensitivity treatment. As part of the statistical analysis the sample of participants was split into two groups based on their risk belief. These two groups were low risk belief which contained 38 participants (37%), and medium/high risk belief which contained 66 participants (63%). As their main occupation 44% op participants were full-time students, 35% were working as paid employees, 12% were working self-employed, 5% were part-time students and the remaining 4% were not working because of several different reasons. A summary of the continuous variables can be seen in Table 2.

Table 2. Summary of the variables that were measured on a numerical scale or were derived from numerically recorded data.

Statistic	Mean	St. Dev.	Median	Pctl(25)	Pctl(75)	Min	Max	N
simon_effect	59.83	111.29	52.40	−2.49	98.10	−330.29	561.58	104
risk_belief	0.32	1.54	0.70	−1.00	1.40	−3.00	3.00	104
behavioural_intention	−0.41	1.85	−0.5	−2	1.5	−3	3	104
pay	21.37	62.25	10.00	3.00	20.00	0.00	600.00	101
expectation	0.56	1.67	1	−1	2	−3	3	104
protection	−0.17	1.60	0	−2	1	−3	3	104
exposure	2.10	1.17	2	2	3	−3	3	104
experiences	−0.54	1.84	−1	−2	1	−3	3	104

Summary of the variables that were measured on a numerical scale.

4.2 Correlations

Before going into the actual analyses of effects of variables upon one another using regressions and t-tests, let's first look at the correlations in the collected data between the constructs that were used. Table 3 shows these correlations, which give insight in which variables are correlated. These will be useful when interpreting certain relationships between variables in the next section.

Table 3. Correlations between the measured constructs (see Appendix subsection 1 for correlations involving willingness to pay and income).

	simon_effect	sensitivity	risk_belief	risk_belief_split	behavioural_intention	pay	expectation	protection	exposure	experiences	education	age	gender	income	referral
simon_effect	1	-0.02	0	-0.06	0.07		-0.13	0.06	-0.01	-0.23	-0.10	0.18	0.07		-0.02
sensitivity	-0.02	1	0.62	0.55	-0.54		-0.08	-0.10	-0.12	-0.05	-0.12	-0.04	-0.23		0.05
risk_belief	0	0.62	1	0.88	-0.85		0.15	0.06	0.01	0.21	-0.13	0.25	-0.06		-0.21
risk_belief_split	-0.06	0.55	0.88	1	-0.74		0.12	0.07	0.01	0.21	-0.16	0.12	-0.08		-0.15
behavioural_intention	0.07	-0.54	-0.85	-0.74	1		-0.22	-0.14	-0.06	-0.20	0.06	-0.26	0.02		0.30
pay						1									
expectation	-0.13	-0.08	0.15	0.12	-0.22		1	-0.05	0.39	0.63	-0.10	0.05	0.23		-0.25
protection	0.06	-0.10	0.06	0.07	-0.14		-0.05	1	-0.03	-0.03	-0.01	0.28	0.26		-0.17
exposure	-0.01	-0.12	0.01	0.01	-0.06		0.39	-0.03	1	0.48	-0.11	-0.04	0.07		-0.28
experiences	-0.23	-0.05	0.21	0.21	-0.20		0.63	-0.03	0.48	1	0.05	-0.05	0.07		-0.22
education	-0.10	-0.12	-0.13	-0.16	0.06		-0.10	-0.01	-0.11	0.05	1	0.21	0.09		0.14
age	0.18	-0.04	0.25	0.12	-0.26		0.05	0.28	-0.04	-0.05	0.21	1	0.37		-0.21
gender	0.07	-0.23	-0.06	-0.08	0.02		0.23	0.26	0.07	0.07	0.09	0.37	1		-0.27
income														1	
referral	-0.02	0.05	-0.21	-0.15	0.30		-0.25	-0.17	-0.28	-0.22	0.14	-0.21	-0.27		1

N = 104. The columns of income and willingness to pay contain missing values.

4.3 Results of Analysis

What follows are the results of the statistical analyses of the collected data with the hypotheses of interest in mind. For some relationships between variables additional discoveries were made. These additional findings are also reported in this section. This section is structured around the following four dependent variables: inhibitory control, risk belief, behavioural intention and willingness to pay. A summary of results can be seen in Table 5, but should not be seen as a complete picture of all the intricacies discovered in the analyses.

Inhibitory Control. Inhibitory control was found to be neither practically, nor statistically significantly affected by risk belief or protection belief (H1a and H1b not supported)(see Appendix subsection 2). Information sensitivity conditions also did not differ significantly in inhibitory control ('Simon effect') (two-sample t-test: t(101.84)=0.20724, p=0.8362, 95% confidence int.= [-38.55223 47.54779]). The low information-sensitivity treatment group (M=62.296) had on average a 4 milliseconds smaller Simon effect than the high information-sensitivity treatment group (M=57.798).

Also two groups were created by splitting the sample on grounds of either having low risk belief or medium/high risk belief and were tested for an effect on inhibitory control. Only a statistically insignificant difference of 13 milliseconds was found between the low risk belief group (M=68.036) and the medium/high risk belief (M=55.106) (two-sample t-test: t(83.044)=0.5825, p=0.5618, 95% confidence int.= [-31.21748, 57.07602]).

Table 4 shows the model that appeared best from the hypothesized factors of influence. Protection is left out, as it was found to worsen the explanatory power (R^2_{adj}) of the model while adding extra complexity (higher Akaike Information Criterion (AIC)). Since only the confidence interval of age is bounded from zero (its coefficient values can be said to only be positive with 95% confidence) it seems to be the only factor that reliably predicts inhibitory control (see Figure 5 for a visualization of this relationship and other relationships that were mentioned).

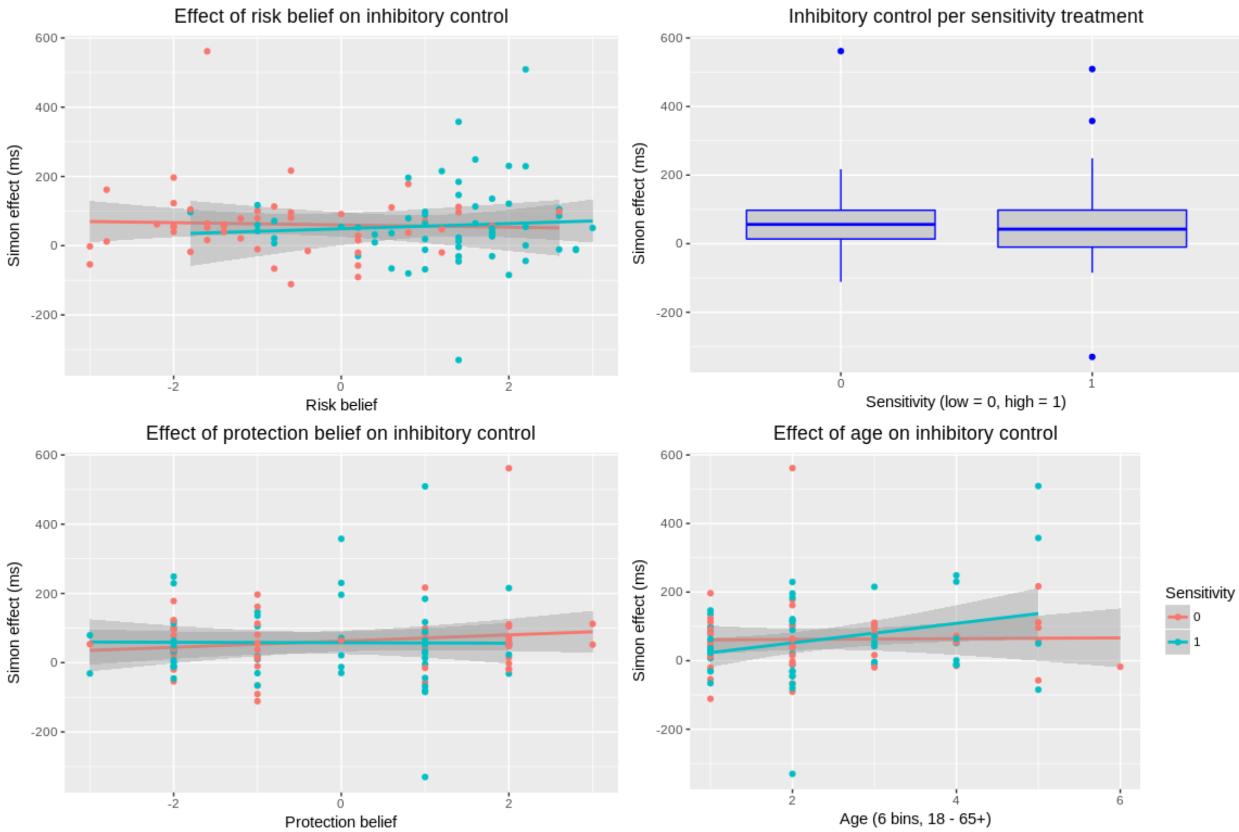

Fig. 5. Figures showing the effects of risk belief (upper left), information sensitivity (upper right), protection belief (bottom left) and age (bottom right) on inhibitory control (measured in the form of the 'Simon effect'). The two lines represent the effect for each information-sensitivity treatment (low sensitivity = 0, high sensitivity = 1).

Table 4. Best hypothesized model predicting inhibitory control (see Appendix subsection 2 for additional diagnoses).

Explanatory variable	Coefficient	St. Error	95% Confidence Interval
Constant	79.55	47.14	[-13,98, 173.08]
Risk belief	-7.00	9.69	[-26.22, 12.22]
Sensitivity	6.67	28.65	[-50.17, 63.51]
Age	19.74*	9.06	[1.78, 37.71]
Education	-10.29	6.61	[-23.40, 2.82]
Linear model. N=104. Residual std. Error: 110.3 (df=99) Adjusted R2: 0.018. F: 1.481 (df=4; 99). Confidence intervals calculated for t-distribution.			
*p<0.05			

Risk Belief. Because of a gap in risk belief scores it was possible to split the participants into either a low risk belief group or a medium/high risk belief group (see Appendix subsection 3). The model where the 'continuous' risk belief was predicted by information-sensitivity treatment condition had a much better fit (R^2_{adj}=0.379) than when the split risk belief was predicted similarly (R^2_{adj}=0.301). Therefore split risk belief has the disadvantage over 'continuous' risk belief.

A very significant positive effect of information-sensitivity treatment on risk belief was found (H2a confirmed). Risk belief is two points higher on the 7-point Likert-type scale for high information sensitivity compared to low information sensitivity. Protection belief did not have a significant effect on risk belief overall, but did have a practically and statistically significant positive effect for those in the low information sensitivity group only (H2b unconfirmed but partly the opposite confirmed), with about one point rise in risk belief per four points of protection belief. This effect might be explained by the correlation of protection belief to other factors, such as a particularly privacy aware group with for example high exposure to privacy messaging. This interaction would yet have to be confirmed. Experienced frequency of personal privacy violations does have a mildly practically significant and statistically significant positive effect by itself on risk belief (H2c confirmed). Each 5-6 points higher on the 7-point scale of frequency of experienced personal privacy violations adds on point in risk belief. Exposure to messaging about privacy vulnerabilities was not found to have any practical nor significant effect on risk belief (H2d not supported). Education was also not found to have any significant effect on risk belief by itself (H2e not supported) (see Appendix). Age was found to indeed have a practically and statistically significant positive effect on risk belief (H2f confirmed). The effect of only age on risk belief (without controlling with other variables) was found such that when age would rise about 35 years (almost 3.5 bins) the risk belief is increased by one point on its 7-point scale. Figure 6 shows the relationships which were found to be significant.

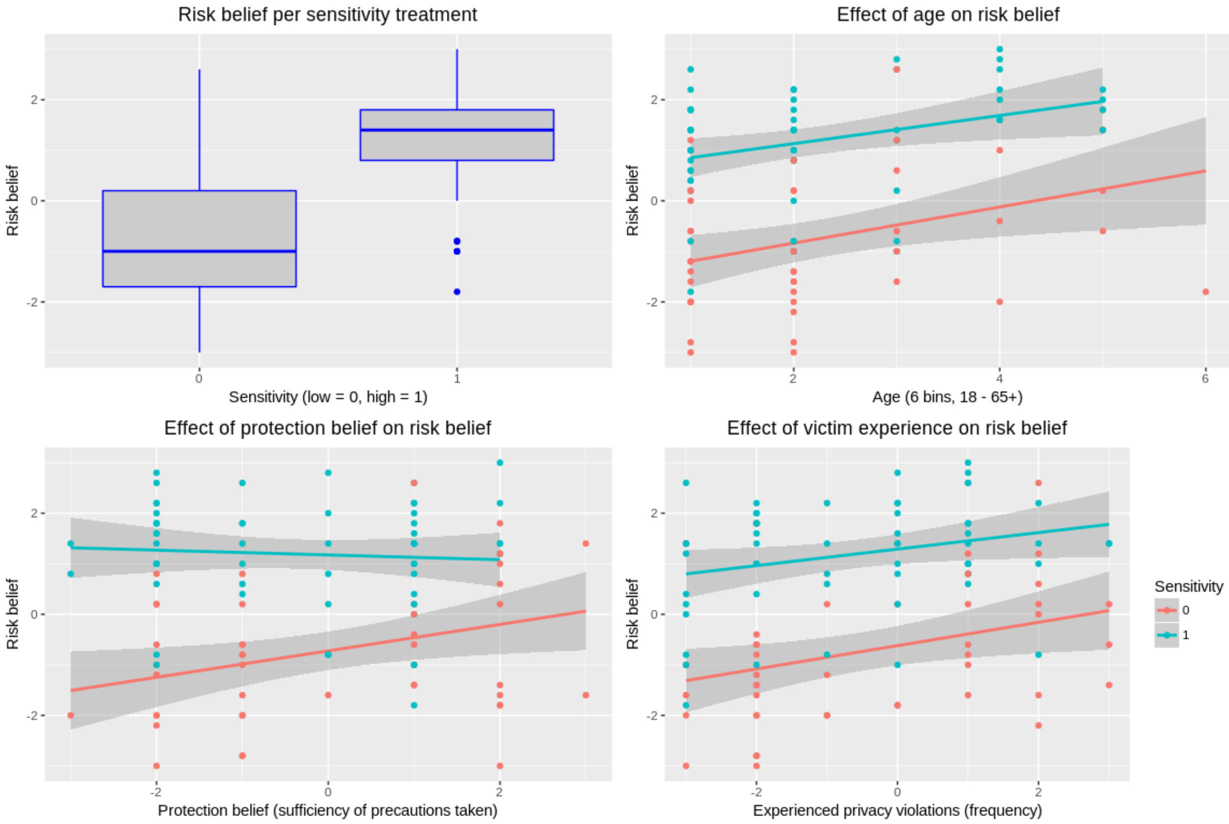

Fig. 6. The effects of sensitivity (upper left), age (upper right), protection belief (bottom left) and experienced privacy violations (bottom right) on risk belief. The two lines represent the effect for each information-sensitivity treatment (low sensitivity = 0, high sensitivity = 1).

While it appears that privacy risk belief increases with age, another explanation might be that given a slice in time older people will always understand less of privacy violations and so have a higher risk belief. Exposure to media content about information misuse to was not found to have any significant effect on risk belief, but this only measured the frequency of exposure during the last year and not life-time exposure. It could be a possible explanation that older people are generally less 'tech savvy' so to say and therefore have a higher risk belief. No measure of technical knowledge or knowledge on information management practices was included in this study. However, a certain subpopulation that may be taken to have more knowledge in this field was included: the participants who were lead to participate by privacy advocacy organisation Bits of Freedom. In addition to their knowledge, the Bits of Freedom referral group might have a relatively high risk belief as well as high age, which could cause any regression on the whole sample to falsely report an effect of age on risk belief.

To see if this is the case, first it was established whether or not the age in groups significantly differed. There was a significant difference of age between the three different subpopulations at the $p<.05$ level [$F(2) = 19.284$, $p = 8.063*10^{-8}$]. Post hoc comparisons using the Tukey HSD test indicated that the mean age (expressed in bins of about ten years each) for the Bits of Freedom lead group ($M = 3.19$, $SD = 0.10$) was significantly different from the last year Bachelor of Arts class ($M = 1.17$, $SD = 0.39$), amounting to a difference between means of almost 20 years (95% CI [1.25, 2.79] also expressed in bins). The mean age also differed significantly between the Bits of Freedom ($M = 3.19$, $SD = 0.10$) and the 'Other' leads ($M = 2.27$, $SD = 1.34$), which is a difference of about 9 years (95% CI [0.28, 1.56]). The difference between Other and the BA class was also significant, with a difference of almost 11 years (95% CI [0.43, 1.77]).

From the difference in age between the groups it might well be that interpretation of any regression on the whole sample would falsely suggest that a cause for variation in risk belief is age. To check if even within these three subpopulations there could be an effect, the risk belief data are plotted per age group for each subpopulation (see Figure 7). From the two upper effect plots it becomes clear that within the lead groups 'Bits of Freedom' and 'Other' there would be an effect of age on risk belief. The effect for the last year Bachelor of Arts class seems to be very dependent on information-sensitivity treatment, but it is comprised of only participants between 18-34 years old. Moreover, this group suffers from very little data points in the low sensitivity condition compared to the other groups. Thus not much can yet be said from the collected data on this group only. From the two lower figures the effect of age on risk belief seems more reliable and steadily climbing for the Bits of Freedom group than for the Other group, but only with more participants than the current study this assumption could tested reliably. From the above discussion it follows that the conclusion of risk belief increasing with age still seems valid so far.

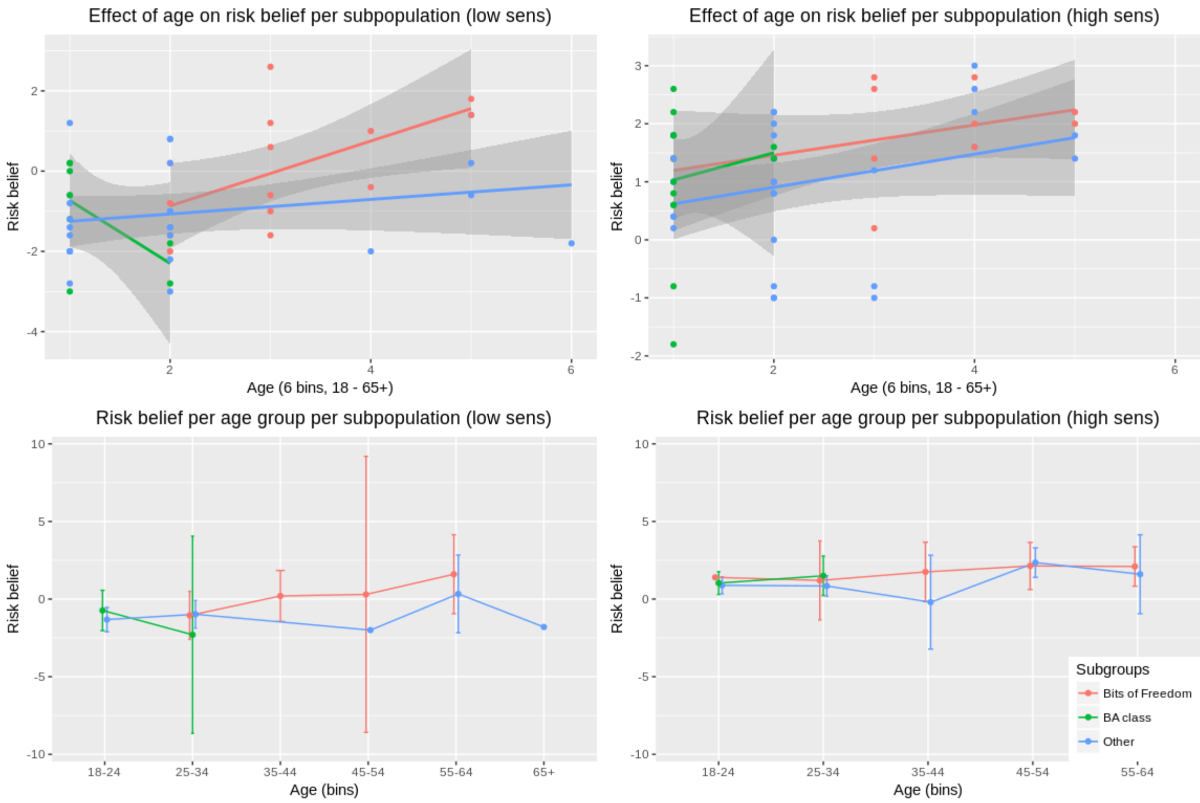

Fig. 7. The effects of age on risk belief for the low information-sensitivity treatment (upper left) and high information-sensitivity treatment (upper right). Thereunder the mean risk belief per age group for the low information-sensitivity treatment (bottom left) and high information-sensitivity treatment (bottom right) protection belief (bottom left), including 95% confidence intervals.

Behavioural Intention. Behavioural intention was hypothesized to be predicted by risk belief and by age. Additionally to checking these hypotheses some mediatory relationships were found. Risk belief was found to have a one-on-one positive effect on behavioural intention (H3a confirmed)(see Figure 8). Risk belief was also found to be the mediator between the information sensitivity and behavioural intention. Information sensitivity had no direct effect on behavioural intention when risk belief was included as a mediator (see Appendix subsection 4).

Age did seem to have an effect on behavioural intention, but from the results of the effect of age on risk belief (H2f) it is more likely that risk belief mediates between age and behavioural intention. This mediation was indeed found to be the case, with no significant direct effect of age on behavioural intention left (see Appendix 1). Which means that H3b is probably contradicted and it can be added that age has only an indirect effect.

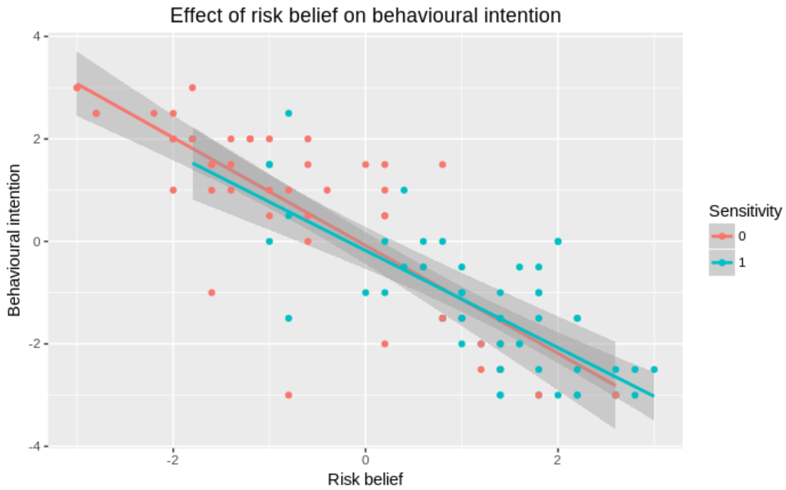

Fig. 8. Effect of risk belief on behavioural intention, per information-sensitivity treatment (low sensitivity = 0, high sensitivity = 1).

Willingness to Pay for Non-Disclosure. Risk belief, age and protection belief were hypothesized to affect willingness to pay (WTP). The median WTP was on 10.00 euros and the mean on 21.37 euros with a minimum of 0 and a maximum of 600 euros. The effect of risk belief on WTP was found to be positive and significant, adding 41-53 euro cents per point on the 7-point risk belief scale (H4a confirmed)(see Figure 9). Unlike with behavioural intention, information sensitivity had no significant effect on WTP on its own. Thus risk belief can't be said to be mediator between information sensitivity and WTP. Still risk belief does affect willingness to pay, but not as mediator for information sensitivity unlike with behavioural intention. One explanation for this could be that another factor forming risk belief exerts this influence instead or at least more than information sensitivity. While income was not found to have a direct effect on WTP, it was found to significantly moderate the effect between risk belief and WTP. For every 500 euros more in income, each point on the 7-point risk belief scale is worth 8 euro cents more when affecting WTP.

Age was found to have a positive effect on WTP of about 23-58 euro cents per about 10 years (1 bin). In fact, the significant interaction with information sensitivity reveals that each about 10 years of age will only add about 8 euro cents to WTP if the information-sensitivity treatment is high and 58 euro cents if it is low. These results cannot be interpreted without first controlling for two other factors. Firstly, income was found to mediate between age and WTP or to moderate this relationship. Age was also found to have a positive effect on income, as can be expected. Secondly, it was found that risk belief is a strong mediator between age and WTP. This was somewhat expected because risk belief was also found to mediate between age and behavioural intention. Thus, H4b is contradicted to the extent that it can be assumed that clearly risk belief is a mediator between age and WTP, and income also appears to have a similar role.

The seeming overall effect of protection belief on WTP of about 17 euro cents per point on the 7-point protection scale was not found to be significant. When controlling for information sensitivity the finding was that per one point protection belief on a 7-point scale participants were willing to pay 42 euro cents more, unless the sensitivity of the information was high which canceled out the effect of protection belief on WTP. The group which received the low information-sensitivity treatment had a mean protection belief (M= -0.043) that was 0.30 higher than the low information sensitivity group (M= -0.345), but it was not significantly different (two-sample t-test: t(90.885)=0.92916, p=0.3553, 95% confidence int.= [-0.3436038, 0.9475564]). Thus, H4c is partly unconfirmed and partly contradicted (more details on the analyses of WTP can be found in Appendix subsection 5). See Figure 9 for a visual representation of the linear model for protection belief and WTP.

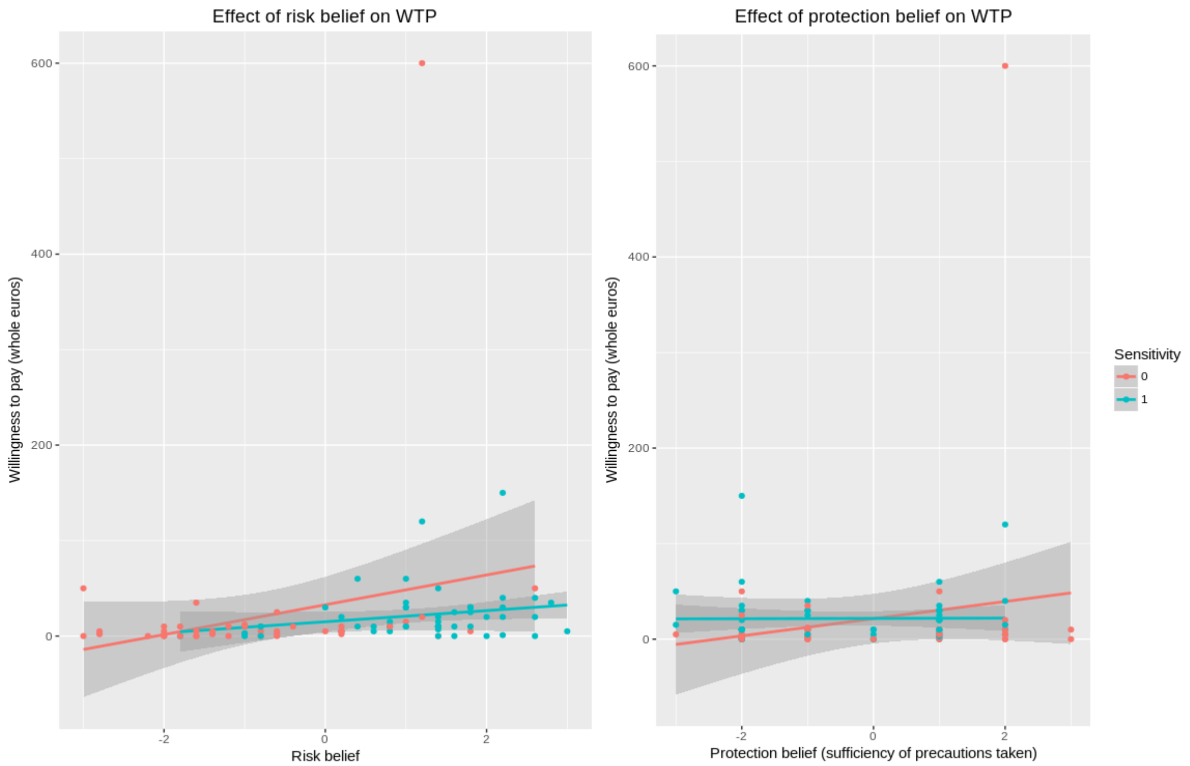

Fig. 9. The effects of risk belief (left) and protection belief (right) on willingness to pay (WTP). The two lines represent the effect for each information-sensitivity treatment (low sensitivity = 0, high sensitivity = 1).

Table 5. Summary of the results from testing the original hypotheses, including notes on mediation or moderation relationships that were found.

Number	Independent variable	Significant effect (size)[1], and notes →	Dependent variable	Hypothesized effect
1		**Inhibitory Control**		
a	Risk belief	none	Inhibitory control	- (not supported)
b	Protection belief	None Note: age → inhibitory control +	Inhibitory control	+ (not supported)
2		**Risk Belief**		
a	Information sensitivity	+ (1.913)	Risk belief	+ (supported)
b	Protection belief	+ (0.262) Note: low sensitivity only	Risk belief	- (partly contradicted)
c	Experiences of privacy violation	+ (0.174)	Risk belief	+ (supported)
d	Exposure to messaging about privacy vulnerabilities	none	Risk belief	+ (not supported)
e	Education	none	Risk belief	+ (not supported)
f	Age	+ (0.288)	Risk belief	+ (supported)
3		**Behavioural Intention**		
a	Risk belief	- (1.019) Note: risk belief found to mediate between sensitivity and behavioural intention	Behavioural intention	- (supported)
b	Age	- (0.366) Note: but risk belief found to mediate: age → risk belief +(0.288)	Behavioural intention	- (contradicted)
4		**Willingness to Pay for Non-Disclosure**		
a	Risk belief	+ (0.407)	Willingness to pay	+ (supported)
b	Age	+ (0.233) Note: but probable income interaction / mediation, and risk belief found to mediate: age → risk belief +(0.288)	Willingness to pay	+ (contradicted)
c	Protection belief	+ (0.420) Note: low sensitivity only	Willingness to pay	- (partly contradicted)

Notes: + is a positive effect, - is a negative effect. Variables have not been normalized, effect sizes should be interpreted for the scales that were used. "a → b" means "the effect of variable a on variable b".
[1]Significant as explained in Section 3.2 as at least a practically significant effect size with a 95% CI bounded away from zero. Also $p<0.05$ for most of these effects.

5 Discussion

5.1 Theoretical and Practical Implications

The results of this study should be interpreted in light of the discussed theory to learn more about their meaning and grasp their implications for the theories that were found in the literature. The most noteworthy results from the perspective of theory are discussed in this section.

From a combination of studies from the behavioural economics literature and the literature on online privacy trade-offs discussed in Section 1 and 2, it was hypothesized that inhibitory control would change based on risk beliefs and other contextual factors in online privacy trade-off situations. Neither risk belief, belief about general protection sufficiency or the sensitivity of the information being traded seemed to have any significant effect on inhibitory control in this study. It might be that the effects are just too small to notice based on one hypothetical trade-off scenario or that there is no effect of contextual factors on the magnitude of the loss of cognitive control. In that case it might just be that changing the parameters of a privacy scenario does not matter in practice, and that any ego depletion would remain constant after it is known that the scenario involves a privacy dimension.

In fact, research on the factors that affect information disclosure found that people actually shared less information in an online decision-making process if privacy (a privacy policy) was only as little as mentioned either positively or negatively (Marreiros et al., 2017). So, as soon as people are aware that a trade-off involves privacy, they share less information. But if people are aware of a privacy dimension their thoughts should, according to the hypotheses of this research paper, become more burdened, hence creating cognitive scarcity. Thus, if privacy concerns tax cognitive function in a decision-making process it should have been the case that people started sharing more, not less personal information. Nevertheless, it might still be possible that in the scenario used by Marreiros et al. (2017) cognitive scarcity was indeed caused by the awareness of the privacy aspect of the trade-off. But that this awareness then for example created a higher sense of risk belief which outweighed any of the effect of the cognitive scarcity on information disclosure.

Inhibitory control was found to be worse for higher age groups, by proxy of a larger Simon effect. The negative influence of age could be expected from an effect that is derived from reaction time. So this finding does not necessarily mean that older people will be prone to sharing more sensitive information than younger people, even though exhausting inhibitory control was found to positively affect information disclosure behaviour (Veltri & Ivchenko, 2017). This conclusion cannot be drawn because the Simon task is just used as a proxy to measure inhibitory control. In fact, Salthouse, Toth, Daniels, Parks, Pak, Wolbrette, & Hocking (2000) found a similar mediating effect of age increasing reaction time in their testing of the higher-order cognitive function of cognitive flexibility. Additionally, Veltri & Ivchenko (2017) found no effect of age on information disclosure behaviour. However, from this study it becomes clear that age does have a positive effect on risk belief, which then also influences behavioural intention and most probably also actual choice behaviour in online privacy trade-offs (Krasnova et al., 2010). As such, higher age may actually result in generally lower information disclosure.

The frequency of having been a victim of privacy violations (‘experienced privacy violations’) was not found to affect risk belief in an earlier study (Malhotra et al., 2004). In this study however, it seems that experienced privacy violations have a small positive effect on risk belief. There is no clear explanation for why this effect is suddenly found. It could simply mean that people who have been the victim of privacy violation often have increased trauma, or that the experiences feed the availability heuristic similarly to media exposure. But perhaps there is a correlation between exposure to privacy vulnerability messaging or being a ‘privacy nerd’ and experiencing more violations, because the tolerance is less high and the violations are noticed more often. This speculation would still have to be tested. It does not help to see that exposure to vulnerabilities did not seem to have any significant effect on risk belief in this study.

Additionally, protection belief had a substantial effect on risk belief and willingness to pay for non-disclosure, but only for the low information-sensitivity treatment. The cause of this treatment interaction might have been that when participants were answering the question about their general protection sufficiency, the scenario anchored in their minds could have influenced their answer. This would result in a higher protection belief for the group with low information-sensitivity treatment, and a lower protection belief for those who received the high information-sensitivity treatment. While this difference between treatments was indeed found, it was rather small and not statistically significant. Nonetheless, the existing difference in protection belief between high and low information sensitivity treatment groups could still be a plausible explanation for part of the unsuspected interaction. However, as stated above, similar interaction of the treatment was found in the effect of protection belief on risk belief. Then, it would be a more likely hypothesis that the anchoring of low information sensitivity might have caused more variation in the answers for protection belief, as opposed to the anchoring of high information sensitivity. Further research could go into the role of protection belief and how information sensitivity affects it.

The roles of risk belief as a mediator between sensitivity and behavioural intention, age and behavioural intention, and between age and willingness to pay have all been supported by this research. This amends an earlier finding by Malhotra et al. (2004) that age affects behavioural intention directly. In fact the mediation of risk belief between age and behavioural intention is probably the cause of the seeming effect of age in behavioural intention. Also, the role of risk belief as a mediator between age and willingness to pay is quite a new discovery. This mediator relationship even seems to hold somewhat when income is controlled for.

A quite unusual inclusion in the psychological model of online privacy trade-offs is willingness to pay (WTP). One of the expectations was that it could function as kind of an inverse alternative to behavioural intention. Indeed risk belief was found to affect WTP, but the effect size has less body because it is expressed in tens of euro cents only. An important difference between behavioural intention and WTP is that risk belief could not be seen as a mediator between sensitivity and WTP. In fact sensitivity did not seem to affect WTP at all, while risk belief still did affect WTP. Additionally, income seems to moderate the relationship between risk belief and WTP slightly positively. A similarity between behavioural intention and WTP is that age was found to affect both in quite similar amounts and was mediated through risk belief for both. Additionally from the results it becomes apparent that the effect of protection belief on WTP is mediated by risk belief, but possibly only for low risk belief. This could be assessed further in additional research. All characteristics considered, WTP looks to be somewhat less sensitive than the construct of behavioural intention, but it may very well be used instead of behavioural intention in situations where money is a more practical measurement than 5 questions about risk belief.

The point could be raised that the differences between the three subpopulations that participated in the study (leads from Bits of Freedom, the BA class and others) actually make up some of the measured effects. In that case the effects that were found might not exist inside of these participant groups. Indeed the three groups of participants from different leads that were tested differed in size and had some significantly different demographics and results (see Section 4.1 and Section 4.3 on ‘Risk Belief’). However, the assumption of the group differences being the only cause of the overall effects was tested for the most obvious candidate of this fallacy: the finding that age increased risk belief. It was concluded that this effect was present within at least two of the three different subpopulations as well, but that research with a larger number of participants would be necessary to more reliably confirm this conclusion (see Section 4.3 on ‘Risk Belief’).

Finally, the parts of constructs that before had only been used to measure general risk belief and behavioural intention, actually performed very well when they were adapted to measure risk belief and behavioural intention specific to the context of a certain trade-off. Further research should be undertaken to determine the precise statistical reliability of these newer scales. Nevertheless, the fact that they performed as expected in the current study opens new doors for their use in measuring contextual constructs in situations of privacy decision-making.

5.2 Limitations and Recommendations

This research project had some limitations that should be addressed. First of all, one of the theories on which this research builds lacks replication (Dean et al., 2017; Carvalho, Meier, & Wang, 2016; Wicherts & Scholten, 2013; Mani et al., 2013b). Thus far, only Mani et al. (2013) have been able to demonstrate that probably pre-existing and situational financial worries depending on the amount of income, and activated by economic trade-offs, can cause cognitive scarcity.

Besides that, the methodology of this research may have produced results that could have been more adequate or accurate. The fact that no effect of risk belief or information sensitivity on inhibitory control was found in this study, might have been caused by one hypothetical scenario simply being too little to induce any or enough cognitive scarcity to measure a significant difference. Also, getting to know the rules and doing training examples at the start of the Simon task in this research might have distracted the participants from any privacy worries that the scenario might have induced. Therefore it would be beneficial for a follow-up study to make use of several scenario’s neatly woven into the Simon task. This would neutralize for a large part the distractions and limited scenario power. Also this comes closer to the methodology of the study by Mani et al. (2013a).

Additionally, being explicit about instructing participants to think about the scenario while doing the cognition test and making them aware that they have to come up with a choice after the cognition test, might induce a larger effect of worry on the test performance. It might also be more realistic. When a privacy choice has to be made in real life (e.g. going to make an account for an online service), this is often accompanied by actually having to disclose personal information (e.g. filling in telephone number and email address in the same form). The fact that decision-making processes often happen at the same time of information disclosure in real life, was not captured well enough in the methodology of this study.

Also, the conditions of the trials in the Simon task used in the current study (congruent or incongruent) were chosen at random for every trial. This resulted in both different ratios of the number of congruent versus incongruent trials, and in different orders of congruent and incongruent trials during the tests. This might have caused extra and unnecessary variance between participants. This possible disadvantage was partly countered by using the “Simon effects” as a measure of inhibitory control, instead of separately using the average reaction times for the congruent and incongruent trials. But any follow up study would be advised to get rid of this extra variance by using a fixed random order and a 50/50 ratio of congruent and incongruent trials. Then it also becomes more sensible to at least try to use the average reaction times as a measure of inhibitory control in addition to the Simon effect. Mani et al. (2013) used these reaction times instead of the Simon effect. On a different note, it might be that the Simon effect does not appropriately measure inhibitory control, but this would be part of another discussion in the field of cognitive psychology.

Moreover, other measures and sources of data could be used as well to substitute the Simon effect or even inhibitory control. While in this study inhibitory control was used to as a proxy to measure cognitive bandwidth, a next experiment might try to look for any influence on people’s fluid intelligence or working memory. However, it remains to be seen whether the method of using scenario’s is a worthwhile approach due to the probably limited effect. Instead could be opted for a more holistic approach where the effect of pre-existing privacy concern on actual information-disclosing behaviour is tested directly. If you want to know if privacy concerns during online decision-making actually influences online privacy decision-making, then the most reliable way to test it is to measure actual behaviour. To that end, pre-existing data that companies or governments have already collected or collect in their business with their users could be used for the purpose of such research. Also, the willingness to pay that users have expressed through actual payments when choosing for a service could then be linked to the boxes they ticked in the registration process.

Ultimately, the main research question and the two subquestions were formulated to make the research quite exploratory in nature. Now that the idea of privacy in decision-making processes possibly causing cognitive scarcity and perhaps even a ‘privacy trap’ is out there, approaches with a different angle could be thought of to research this relationship. Firstly, a slightly different approach might be taken to investigate if privacy concerns could cause cognitive scarcity. The differences between inherently distinct participant groups could be used to interpret a difference in cognitive bandwidth between these groups. In Sections 4 and 5.1 the differences between the subpopulations of participants that took part in this study were demonstrated and discussed. The three subpopulations were found to be distinct in some of their demographics and in some other measurements, such as their level of risk belief. These differences could be taken advantage of to make for a more reliable and less troublesome methodology. Specifically, future research might take two different populations as ‘treatment’ groups, for example users of a game-related website and users of a privacy-related website. Then for both groups the cognitive bandwidth would be measured using a test. The difference in cognitive bandwidth between the groups could then be compared. When starting from the hypotheses that privacy concerns limit cognitive bandwidth, then the people on the privacy-related website would have lower cognitive bandwidth than those on the game-related website when also controlling for other factors such as age. This method would avoid having to use (fictive) scenario’s, because it relies on the already occurring differences between the populations and perhaps their mindset when coming from their respective websites.

Secondly, it might be interesting to find out if the effect of being aware of the privacy dimension of a trade-off on cognitive bandwidth is overshadowing any change in cognitive bandwidth by the contextual factors that were researched in this project. One approach to that would be to first measure if there is any change in cognitive bandwidth as a result of only ‘activating’ the dormant general privacy concerns (Marreiros et al., 2017).

Thirdly, a more qualitative empirical approach could be taken to discover the impact of privacy on peoples’ daily lives. This approach would involve more of a qualitative touch to discover if privacy concerns and thoughts are salient in peoples daily lives and if their salience is affected by factors such as general privacy concern or more contextual factors. In economic research of this kind, it was discovered that thoughts about money or monetary cost are more easily triggered, arise more often rather unprompted, are more persistent, and are more strongly associated to related words for poorer people (Shah, Zhao, Mullainathan, & Shafir, 2018; Schilbach, Schofield, & Mullainathan, 2016). It remains to see whether these particular characteristics also apply to thoughts about information privacy, and whether this is related to general privacy concerns or other factors.

6 Conclusion

This research project has been trying to connect theories and findings from both the research on online privacy trade-offs and economic trade-offs. The main question was whether a ‘privacy trap’ exists, alike a ‘poverty trap’. Specifically it was hypothesized that contextual factors within online privacy trade-offs would influence any loss in cognitive bandwidth that a privacy trade-off might cause. This loss in cognitive bandwidth could consequently lead to more information disclosure. Cognitive bandwidth was measured by proxy of inhibitory control. To make the hypothesis workable, the two subquestions asked which factors influence the possible cognitive scarcity, in what way, and to which degree? Certain measurable constructs, such as risk belief, were fleshed out to operationalise these factors. In this study these factors were not found to have an effect on inhibitory control. Though, it was found that age probably affects the level of inhibitory control. Additionally, support was found for some relationships between privacy decision-making constructs that were previously not found in other studies. Also the view upon some relationships between constructs within privacy decision-making may be amended, because some mediation or moderation effects were found. Furthermore, some measurement scales that had earlier been used only to measure general beliefs and intentions connected to online privacy trade-offs, were in this study found to perform well when adopted to measure beliefs and intentions specific to the context of a certain online privacy trade-off. Also, this research has produced input on the limitations of some methodological approaches and formed recommendations for further research on this specific topic of online privacy trade-offs affecting cognitive function. In short, this exploratory study into the possible effect of privacy concerns on cognitive bandwidth uncovered some preliminary relationships between variables that affect beliefs and behavioural intentions in online privacy decision-making. Now that the idea of online privacy decision-making affecting cognitive bandwidth has been brought up, the floor is open to anyone to join the search for answers. If privacy concerns are found to be affecting cognitive function, then that would explain a lot of the yet to explain online behaviour of people.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 44.

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

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-92.

Baddeley, A. D., & Hitch, G. (1974). Working memory. In *Psychology of learning and motivation* (Vol. 8, pp. 47-89). Academic press.

Banerjee, A. V., & Mullainathan, S. (2008). Limited attention and income distribution. *American Economic Review*, *98*(2), 489-93.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of personality and social psychology, 51(6), 1173.

Baumeister, R. F., Bratslavsky, E., Muraven, M., & Tice, D.M. (1998). Ego depletion: Is the active self a limited resource?. In *Journal of Personality and Social Psychology*, 74(5), 1252-1265).

Baumeister, R. F., & Heatherton, T. F. (1996). Self-regulation failure: An overview. *Psychological inquiry*, *7*(1), 1-15.

Baumeister, R. F., Vohs, K. D., & Tice, D. M. (2007). The strength model of self-control. *Current directions in psychological science*, *16*(6), 351-355.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the Association for Information Science and Technology, 58(2), 157-165.

Camerer, C. (1998). Bounded rationality in individual decision making. *Experimental economics*, *1*(2), 163-183.

Carvalho, L. S., Meier, S., & Wang, S. W. (2016). Poverty and economic decision-making: Evidence from changes in financial resources at payday. American Economic Review, 106(2), 260-84.

Dean, E. B., Schilbach, F., & Schofield, H. (2017). Poverty and Cognitive Function. In The Economics of Poverty Traps. University of Chicago Press.

Diamond, A. (2013). Executive functions. *Annual review of psychology*, *64*, 135-168.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295-316.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research*, *21*(1), 119-134.

Festinger, L. A. (1957). Theory of Cognitive Dissonance. Stanford, CA: Stanford University Press.

Gigerenzer, G. (2004). Fast and frugal heuristics: The tools of bounded rationality. In D. Koehler, N. Harvey (Eds.), *Blackwell handbook of judgment and decision making* (pp. 62-88). Oxford, UK: Blackwell.

Gigerenzer, G., & Goldstein, D. G. (1996). Reasoning the fast and frugal way: models of bounded rationality. *Psychological review*, *103*(4), 650-669.

Gigerenzer, G., Todd, P. M., the ABC Research Group (1999). Simple heuristics that make us smart. New York: Oxford University Press.

Gill, J. (1999). The insignificance of null hypothesis significance testing. Political Research Quarterly, 52(3), 647-674.

Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on New security paradigms workshop (pp. 133-144). ACM.

Jurado, M. B., & Rosselli, M. (2007). The elusive nature of executive functions: a review of our current understanding. *Neuropsychology review*, *17*(3), 213-233.

Kahneman, D., & Egan, P. (2011). Thinking, fast and slow (Vol. 1). New York: Farrar, Straus and Giroux.

Kahneman, D., Slovic, P., Tversky, A. (Eds.) (1982): Judgment under uncertainty: Heuristics and biases. New York: Cambridge University Press.

Kahneman, D., Tversky, A. (1996): On the reality of cognitive illusions: A reply to Gigerenzer's critique. *Psychological Review*, 103, 582–591.

Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E. (2015, May). Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus. Association for Information Systems.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109-125.

Lezak, M. D., Howieson, D. B., Loring, D. W., & Fischer, J. S. (2004). *Neuropsychological assessment*. Oxford University Press, USA.

Luck, S. J., & Vogel, E. K. (1997). The capacity of visual working memory for features and conjunctions. *Nature*, *390*(6657), 279.
Lyon, G., & Krasnegor, N. A. (1996). *Attention, memory, and executive function*. Paul H Brookes Publishing.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), 336-355.
Mani, A., Mullainathan, S., Shafir, E., & Zhao, J. (2013). Poverty impedes cognitive function. Science, 341(6149), 976-980.
Mani, A., Mullainathan, S., Shafir, E., & Zhao, J. (2013). Response to comment on “Poverty impedes cognitive function”. Science, 342(6163), 1169-1169.
Marreiros, H., Tonin, M., Vlassopoulos, M., & Schraefel, M. C. (2017). “Now that you mention it”: A survey experiment on information, inattention and online privacy. Journal of Economic Behavior & Organization, 140, 1-17.
Miller, E. K., & Cohen, J. D. (2001). An integrative theory of prefrontal cortex function. *Annual review of neuroscience*, *24*(1), 167-202.
Mullainathan, S., & Shafir, E. (2013). *Scarcity: Why having too little means so much*. Macmillan.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.
Salthouse, T. A., Toth, J., Daniels, K., Parks, C., Pak, R., Wolbrette, M., & Hocking, K. J. (2000). Effects of aging on efficiency of task switching in a variant of the trail making test. *Neuropsychology*, *14*(1), 102.
Savage, S., & Waldman, D. M. (2013). The value of online privacy. Working paper. Retrieved from https://dx.doi.org/10.2139/ssrn.2341311.
Schilbach, F., Schofield, H., & Mullainathan, S. (2016). The psychological lives of the poor. American Economic Review, 106(5), 435-40.
Shah, A. K., Mullainathan, S., & Shafir, E. (2012). Some consequences of having too little. *Science*, *338*(6107), 682-685.
Shah, A. K., Zhao, J., Mullainathan, S., & Shafir, E. (2018). Money in the mental lives of the poor. Social Cognition, 36(1), 4-19.
Simon, H. A. (1982). Models of bounded rationality. Cambridge, MA: MIT Press.
Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological review*, *63*(2), 129-138.
Sternberg, S. (2004). Reaction-time experimentation. Psychology, 600, 301.
Suchy, Y. (2009). Executive functioning: Overview, assessment, and research issues for non-neuropsychologists. *Annals of behavioral medicine*, *37*(2), 106-116.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268.
Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20-36.
Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. Computers in Human Behavior, 73, 238-246.
Wicherts, J. M., & Scholten, A. Z. (2013). Comment on “Poverty impedes cognitive function”. Science, 342(6163), 1169-1169.
Ziliak, S. T., & McCloskey, D. N. (2004). Size matters: the standard error of regressions in the American Economic Review. The Journal of Socio-Economics, 33(5), 527-546.
Ziliak, S., & McCloskey, D. N. (2008). The cult of statistical significance: How the standard error costs us jobs, justice, and lives. University of Michigan Press.

Non-Academic References

Forbrukerrådet. (2018, June 27). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Report. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Software Used for Data Analysis

Auguie, B. (2017). gridExtra: Miscellaneous Functions for "Grid" Graphics. R package version 2.3. https://CRAN.R-project.org/package=gridExtra.
Fox, J., & Weisberg, S. (2011). An {R} Companion to Applied Regression, Second Edition. Thousand Oaks CA: Sage. http://socserv.socsci.mcmaster.ca/jfox/Books/Companion.
Hlavac, M. (2018). stargazer: Well-Formatted Regression and Summary Statistics Tables. R package version 5.2.1. https://CRAN.R-project.org/package=stargazer.
Lumley, T., based on Fortran code by Miller, A. (2017). leaps: Regression Subset Selection. R package version 3.0. https://CRAN.R-project.org/package=leaps.

R Core Team (2018). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/.

Revelle, W. (2018). psych: Procedures for Personality and Psychological Research, Northwestern University, Evanston, Illinois, USA. Version 1.8.4. https://CRAN.R-project.org/package=psych.

Venables, W. N., & Ripley, B. D. (2002). Modern Applied Statistics with S. Fourth Edition. Springer, New York.

Wickham, H. (2009). ggplot2: Elegant Graphics for Data Analysis. Springer-Verlag New York.

Wickham, H. (2007). Reshaping Data with the reshape Package. Journal of Statistical Software, 21(12), 1-20. http://www.jstatsoft.org/v21/i12/.

7 Appendix

7.1 Full Correlations

A more in detailed description of the results of the statistical analysis are given here per dependent variable. Table 6 shows a full correlation table to be used for estimating correlations with willingness to pay and income, which in the previous correlation table (Table 3) had missing values. Only the complete rows are shown in this table.

Table 6. Correlation table when including only the 90 complete rows (willingness to pay and income contained NAs).

	simon_effect	sensitivity	risk_belief	risk_belief_split	behavioural_intention	pay	expectation	protection	exposure	experiences	education	age	gender	income	referral
simon_effect	1	-0.09	-0.04	-0.07	0.12	-0.18	-0.14	0.05	0.04	-0.22	-0.03	0.18	0.06	0.05	-0.06
sensitivity	-0.09	1	0.65	0.62	-0.59	0.29	-0.08	-0.11	-0.10	0.02	-0.09	-0.01	-0.27	-0.01	0.01
risk_belief	-0.04	0.65	1	0.88	-0.85	0.37	0.16	-0.03	0.01	0.24	-0.12	0.19	-0.16	0.08	-0.15
risk_belief_split	-0.07	0.62	0.88	1	-0.74	0.35	0.10	-0.04	-0.01	0.20	-0.20	0.04	-0.19	-0.11	-0.08
behavioural_intention	0.12	-0.59	-0.85	-0.74	1	-0.40	-0.21	-0.03	-0.04	-0.22	0.07	-0.14	0.18	-0.13	0.24
pay	-0.18	0.29	0.37	0.35	-0.40	1	0.13	-0.12	0.10	0.24	0.04	0.01	0.06	0.12	-0.05
expectation	-0.14	-0.08	0.16	0.10	-0.21	0.13	1	-0.08	0.37	0.61	-0.17	0.02	0.20	0.07	-0.21
protection	0.05	-0.11	-0.03	-0.04	-0.03	-0.12	-0.08	1	-0.06	-0.07	-0.03	0.21	0.15	0.12	-0.07
exposure	0.04	-0.10	0.01	-0.01	-0.04	0.10	0.37	-0.06	1	0.46	-0.15	-0.09	0.03	0.05	-0.27
experiences	-0.22	0.02	0.24	0.20	-0.22	0.24	0.61	-0.07	0.46	1	-0.06	-0.09	0.03	0.05	-0.15
education	-0.03	-0.09	-0.12	-0.20	0.07	0.04	-0.17	-0.03	-0.15	-0.06	1	0.25	0.08	0.47	0.28
age	0.18	-0.01	0.19	0.04	-0.14	0.01	0.02	0.21	-0.09	-0.09	0.25	1	0.29	0.66	-0.10
gender	0.06	-0.27	-0.16	-0.19	0.18	0.06	0.20	0.15	0.03	0.03	0.08	0.29	1	0.31	-0.17
income	0.05	-0.01	0.08	-0.11	-0.13	0.12	0.07	0.12	0.05	0.05	0.47	0.66	0.31	1	-0.10
referral	-0.06	0.01	-0.15	-0.08	0.24	-0.05	-0.21	-0.07	-0.27	-0.15	0.28	-0.10	-0.17	-0.10	1

N = 90. Rows containing NAs for income and willingness to pay have been removed.

7.2 Inhibitory Control

Two factors where hypothesized initially to have a direct effect on inhibitory control: risk belief and protection belief.

Risk Belief. Neither a practically nor statistically significant effect between risk belief and inhibitory control could be discovered. Moreover, the information-sensitivity treatment does not explain the variance in inhibitory control either. Also there is no interaction found between sensitivity and risk belief which affects inhibitory control. See Table 7 for a summary and comparison of the models from which the above findings were derived.

Table 7. Comparison of three nested models for risk belief predicting inhibitory control (‘simon_effect´) and interaction with information sensitivity.

	Dependent variable:		
	simon_effect		
	(1)	(2)	(3)
risk_belief	−0.021 (−14.024, 13.981)	1.435 (−16.497, 19.367)	−3.274 (−27.248, 20.700)
sensitivity		−7.243 (−62.552, 48.066)	−11.058 (−68.014, 45.899)
risk_belief:sensitivity			10.780 (−25.493, 47.053)
Constant	59.838*** (37.867, 81.808)	63.334*** (28.693, 97.975)	59.927*** (23.331, 96.524)
AIC	1280.27	1282.2	1283.85
BIC	1288.2	1292.78	1297.07
Observations	104	104	104
R^2	0.0000001	0.001	0.004
Adjusted R^2	−0.010	−0.019	−0.026
F Statistic	0.00001 (df = 1; 102)	0.033 (df = 2; 101)	0.135 (df = 3; 100)
Note:			*p<0.1; **p<0.05; ***p<0.01 Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution)

Protection Belief. No significant effect between protection belief and inhibitory control was found. Moreover, sensitivity treatment does not explain the variance in inhibitory control either. Also there is no interaction found between sensitivity and protection, which affects inhibitory control. There is no practical significance due to the size of the confidence intervals and also no statistical significance from both the confidence intervals and the p-values (see Table 8).

Table 8. Comparison of the three nested models for protection belief predicting inhibitory control (‘simon_effect´) and interaction with information sensitivity.

	Dependent variable:		
	simon_effect		
	(1)	(2)	(3)
protection	4.429 (−9.012, 17.870)	4.333 (−9.239, 17.905)	8.977 (−9.920, 27.874)
sensitivity		−3.130 (−46.650, 40.391)	−4.708 (−48.568, 39.151)
protection:sensitivity			−9.644 (−36.875, 17.588)
Constant	60.597*** (39.021, 82.173)	62.296*** (30.233, 94.358)	62.296*** (30.151, 94.441)
AIC	1279.84	1281.82	1283.32
BIC	1287.77	1292.4	1296.54
Observations	104	104	104
R^2	0.004	0.004	0.009
Adjusted R^2	−0.006	−0.015	−0.021
F Statistic	0.417 (df = 1; 102)	0.216 (df = 2; 101)	0.304 (df = 3; 100)
Note:			*p<0.1; **p<0.05; ***p<0.01 Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution)

7.3 Risk Belief

As much as seven factors were hypothesized to have a direct effect on risk belief. The analyses also added extra looked at additional variables where appropriate. From the distribution of risk belief in the sample, it seems doable to split up the participants into either having a low risk belief or having a medium or high risk belief. There is exactly a 'gap' just under the middle of the 7-point Likert-type scale range used for measuring risk belief (see Figure 10). It should also fit better than the median split that was used by Mani et al. (2013) to artificially create a distinction between poor and rich participants. This split risk belief could be used additionally or alternatively to the more continuous risk belief measurement.

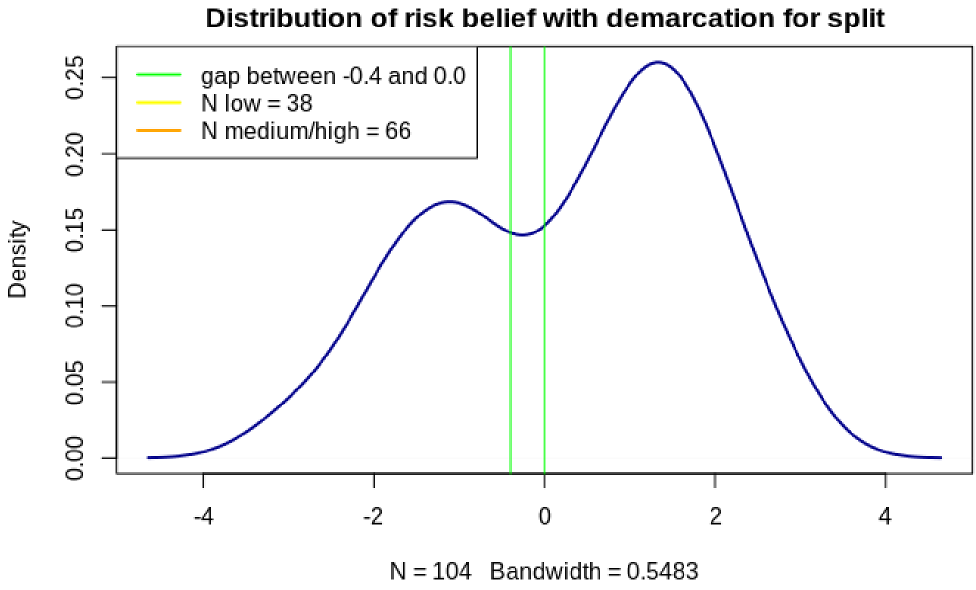

Fig. 10. Distribution of risk belief and the gap where the sample could be split into two groups (low versus medium/high).

Information Sensitivity. There seems to be a statistically and practically significant effect between information sensitivity (the two treatment conditions) and risk belief. Risk belief rises about two points on the 7-point Likert-type scale between low and high information sensitivity. When risk belief is split into a low and medium/high group, then there are also statistically and practically significant effects. But then the effect size shrinks to only about a quarter of the effect size compared to using the 'continuous' risk belief measure as the variable to be explained. The model with the continues risk level as dependent variable also explains more of the variance than the model with binary risk belief as the dependent variable (telling from the R^2 and adjusted R^2). Measuring risk belief continuously should be preferred, at least when dependent relation upon the sensitivity of information is concerned. See Table 9 for the results mentioned in this paragraph.

Table 9. Comparison of the effect of information sensitivity on two different scales of measuring risk belief.

	Dependent variable:	
	risk_belief	risk_belief_split
	(1)	(2)
sensitivity	1.913***	0.537***
	(1.443, 2.382)	(0.381, 0.693)
Constant	−0.723***	0.340***
	(−1.071, −0.376)	(0.225, 0.456)
AIC	339.78	110.88
BIC	347.71	118.82
Observations	104	104
R^2	0.385	0.308
Adjusted R^2	0.379	0.301
F Statistic (df = 1; 102)	63.756***	45.349***

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Protection Belief. There is no significant effect between protection belief and inhibitory control overall, and for the high information sensitivity. There does seem to be a statistically and practically significant small positive effect of protection belief on risk belief in the condition of low information sensitivity. This is further substantiated by adding the interaction between protection and sensitivity treatment to additional models and comparing them. The model with the interaction effects performs much better both on fit and on Akaike's information criterion (AIC) and Beyesian information criterion (BIC) which are lowest for the model including interaction (see Table 10).

Table 10. Comparison of the effect of protection belief on risk belief.

	Dependent variable:		
	risk_belief		
	(1)	(2)	(3)
protection	0.053	0.113	0.262**
	(−0.133, 0.239)	(−0.033, 0.259)	(0.062, 0.461)
sensitivity		1.949***	1.898***
		(1.480, 2.417)	(1.434, 2.361)
protection:sensitivity			−0.309**
			(−0.597, −0.021)
Constant	0.334**	−0.723***	−0.723***
	(0.035, 0.633)	(−1.069, −0.378)	(−1.063, −0.384)
AIC	389.96	339.45	336.94
BIC	397.89	350.03	350.16
Observations	104	104	104
R^2	0.003	0.398	0.424
Adjusted R^2	−0.007	0.386	0.407
F Statistic	0.311 (df = 1; 102)	33.426*** (df = 2; 101)	24.519*** (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Experienced Privacy Violations. The level of previously experienced personal privacy violations does seem to have a positive effect on risk belief with some practical and with statistical significance overall. The effect size for low information sensitivity seems higher on first sight. However, further scrutiny reveals that the interaction between experiences and information sensitivity is negligible. The effect size of the interaction is not of practical significance and its 95% confidence interval is not bounded away from zero (see Table 11), meaning that the effect could be either negative or positive.

Table 11. Comparison of models on the effect of experienced personal privacy violations on risk belief.

	Dependent variable:		
	risk_belief		
	(1)	(2)	(3)
experiences	0.174^{**}	0.198^{***}	0.231^{***}
	(0.015, 0.333)	(0.076, 0.320)	(0.059, 0.403)
sensitivity		1.946^{***}	1.910^{***}
		(1.495, 2.396)	(1.440, 2.381)
experiences:sensitivity			−0.067
			(−0.313, 0.178)
Constant	0.419^{***}	-0.635^{***}	-0.620^{***}
	(0.115, 0.722)	(−0.973, −0.297)	(−0.963, −0.277)
AIC	385.69	331.91	333.61
BIC	393.63	342.49	346.83
Observations	104	104	104
R^2	0.043	0.440	0.442
Adjusted R^2	0.034	0.429	0.425
F Statistic	4.596^{**} (df = 1; 102)	39.735^{***} (df = 2; 101)	26.400^{***} (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Exposure to Messaging about Privacy Vulnerability. The level of exposure to messaging about privacy vulnerabilities does not seem to have any effect on risk belief. The effect in both conditions and in each condition cannot be said to be of practical or statistical significance. Looking at the model wherein interaction with the information-sensitivity treatment was included, this previous suspicion is confirmed (see Table 12).

Table 12. The effect of exposure to messaging about privacy vulnerabilities on risk belief, also checking for interaction with the treatment.

	Dependent variable:		
	risk_belief		
	(1)	(2)	(3)
exposure	0.019	0.123	0.202
	(−0.236, 0.275)	(−0.079, 0.325)	(−0.139, 0.543)
sensitivity		1.949^{***}	2.211^{***}
		(1.476, 2.421)	(1.183, 3.240)
exposure:sensitivity			−0.122
			(−0.546, 0.302)
Constant	0.284	-1.000^{***}	-1.179^{***}
	(−0.329, 0.897)	(−1.573, −0.428)	(−2.023, −0.334)
AIC	390.25	340.32	341.99
BIC	398.19	350.9	355.22
Observations	104	104	104
R^2	0.0002	0.393	0.395
Adjusted R^2	−0.010	0.381	0.377
F Statistic	0.022 (df = 1; 102)	32.722^{***} (df = 2; 101)	21.774^{***} (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Education. The level of education does not seem to have any effect on risk belief. The effect in both conditions together and in each condition separately cannot be said to be of practical or statistical significance. Modeling the interaction with information-sensitivity treatment confirms this (see Table 13).

Table 13. The effect of education on risk belief; and interaction with the information-sensitivity treatment.

	Dependent variable:		
	risk_belief		
	(1)	(2)	(3)
education	−0.115 (−0.288, 0.058)	−0.047 (−0.185, 0.092)	0.099 (−0.133, 0.330)
sensitivity		1.893*** (1.419, 2.368)	3.346*** (1.426, 5.266)
education:sensitivity			−0.225 (−0.512, 0.063)
Constant	1.059* (−0.085, 2.204)	−0.415 (−1.395, 0.566)	−1.377* (−2.948, 0.194)
AIC	388.56	341.33	340.93
BIC	396.5	351.91	354.15
Observations	104	104	104
R^2	0.016	0.387	0.401
Adjusted R^2	0.007	0.375	0.383
F Statistic	1.693 (df = 1; 102)	31.920*** (df = 2; 101)	22.342*** (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Age. The age participants seems to have a positive effect on risk belief. The effect in both conditions together and in each condition separately can be said to be both of practical or statistical significance. Modeling the interaction with the information-sensitivity treatment suggests that this particular interaction effect size is negligible and not of any significance (see Table 14).

Table 14. The effect of age on risk belief; also checking for interaction with the information-sensitivity treatment.

	Dependent variable:		
	risk_belief		
	(1)	(2)	(3)
age	0.288** (0.068, 0.507)	0.318*** (0.151, 0.486)	0.358*** (0.120, 0.595)
sensitivity		1.947*** (1.505, 2.390)	2.126*** (1.244, 3.008)
age:sensitivity			−0.079 (−0.415, 0.257)
Constant	−0.326 (−0.899, 0.248)	−1.461*** (−1.970, −0.953)	−1.552*** (−2.194, −0.911)
AIC	383.74	328.41	330.19
BIC	391.68	338.99	343.41
Observations	104	104	104
R^2	0.061	0.459	0.460
Adjusted R^2	0.052	0.448	0.444
F Statistic	6.614** (df = 1; 102)	42.825*** (df = 2; 101)	28.398*** (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

7.4 Risk Belief

Risk belief and age were hypothesized to have a direct effect on risk behavioural intention. From the analyses some possibilities of mediation where discovered and investigated further. From looking the distribution of behavioural intention is seems arbitrary to split the data into two groups as done with risk belief, because there is no clear gap (see Figure 11). Therefore this 'continuous' measure will be kept in use.

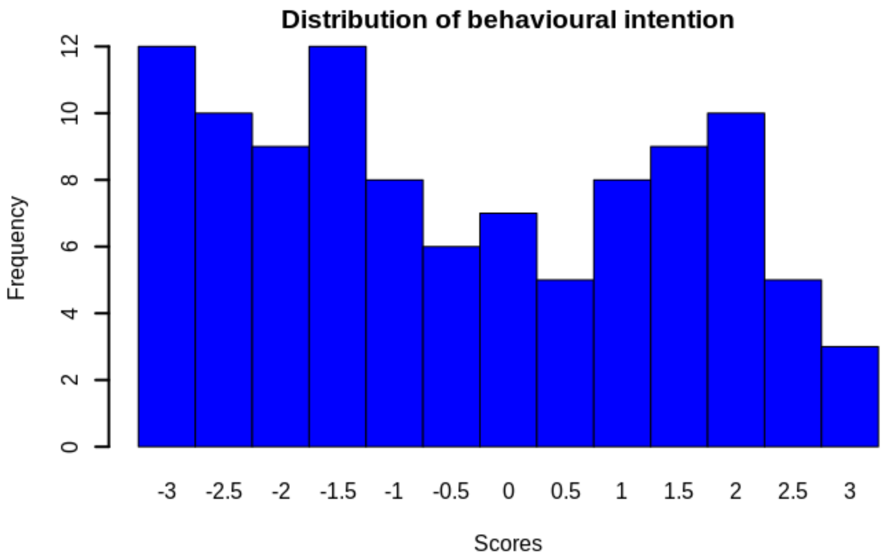

Fig. 11. Distribution of behavioural intention.

Risk Belief. Risk belief seems indeed to have a negative effect on behavioural intention of about one point on a 7 point Likert-type scale. The effect can be said to be both of practical and statistical significance. The interaction with information sensitivity is of no practical or statistical significance taking into account the effect size suggested by the model and its confidence interval (see Table 15). Interesting to note is that when adding information sensitivity to the model this additional variable has an insignificant effect and does not add in explanatory power. This suggests that risk belief is a mediator between information sensitivity and behavioural intention and that there is actually no direct effect between information sensitivity and behavioural intention. To test this hypothesis the method developed by Baron & Kenny (1986) and deployed in a similar setting by Dinev et al. (2013) was used. This analysis confirms that risk belief is indeed a strong mediator and that sensitivity can be said to have no practically and statistically significant direct effect on behavioural intention (see Table 16).

Table 15. The effect of risk belief on behavioural intention; and the interaction with the information-sensitivity treatment.

	Dependent variable:		
	behavioural_intention		
	(1)	(2)	(3)
risk_belief	-1.019^{***}	-1.007^{***}	-1.052^{***}
	$(-1.143, -0.896)$	$(-1.165, -0.849)$	$(-1.263, -0.841)$
sensitivity		-0.062	-0.098
		$(-0.549, 0.425)$	$(-0.599, 0.403)$
risk_belief:sensitivity			0.104
			$(-0.215, 0.423)$
Constant	-0.077	-0.048	-0.080
	$(-0.271, 0.116)$	$(-0.352, 0.257)$	$(-0.402, 0.242)$
AIC	295.77	297.71	299.29
BIC	303.71	308.29	312.51
Observations	104	104	104
R^2	0.720	0.721	0.722
Adjusted R^2	0.718	0.715	0.713
F Statistic	262.936^{***} (df = 1; 102)	130.290^{***} (df = 2; 101)	86.483^{***} (df = 3; 100)

Note: *p<0.1; **p<0.05; ***p<0.01

Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

Table 16. Proving the mediation of risk belief between information sensitivity and behavioural intention in three steps.

	Dependent variable:		
	risk_belief	behavioural_intention	
	(1)	(2)	(3)
risk_belief			-1.007^{***}
			$(-1.165, -0.849)$
sensitivity	1.913^{***}	-1.988^{***}	-0.062
	$(1.443, 2.382)$	$(-2.594, -1.381)$	$(-0.549, 0.425)$
Constant	-0.723^{***}	0.681^{***}	-0.048
	$(-1.071, -0.376)$	$(0.232, 1.130)$	$(-0.352, 0.257)$
AIC	339.78	393.01	297.71
BIC	347.71	400.95	308.29
Observations	104	104	104
R^2	0.385	0.288	0.721
Adjusted R^2	0.379	0.281	0.715
F Statistic	63.756^{***} (df = 1; 102)	41.269^{***} (df = 1; 102)	130.290^{***} (df = 2; 101)
Note:			*p<0.1; **p<0.05; ***p<0.01
	Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.		

Age. Age seems indeed to have a negative effect on behavioural intention. The effect can be said to be both of practical and statistical significance. For low information sensitivity the negative effect size seems to be larger than for high information sensitivity. Further scrutiny reveals that this interaction cannot be interpreted to be practically and statistically significant due to its 95% confidence interval, which is not bounded away from zero (see Table 17). From the analyses of hypotheses H2f, H3b and H3a we can suspect that risk belief might be a mediator between age and behavioural intention. This was tested using the same methodology deployed for mediation testing in H3a. Evidence for strong mediation of risk belief between age and behavioural intention is indeed found. The direct effect of age on behavioural intention is insignificant. This is further supported by the insignificance of the found interaction effect between risk belief and age to predict behavioural intention (see Table 18).

Table 17. The effect of risk belief on behavioural intention; and the interaction with the information-sensitivity treatment.

	Dependent variable:		
	behavioural_intention		
	(1)	(2)	(3)
age	-0.366^{***}	-0.398^{***}	-0.518^{***}
	$(-0.629, -0.104)$	$(-0.615, -0.181)$	$(-0.824, -0.211)$
sensitivity		-2.031^{***}	-2.576^{***}
		$(-2.606, -1.457)$	$(-3.714, -1.437)$
age:sensitivity			0.240
			$(-0.194, 0.675)$
Constant	0.419	1.604^{***}	1.882^{***}
	$(-0.267, 1.106)$	$(0.945, 2.263)$	$(1.054, 2.710)$
AIC	420.98	382.52	383.3
BIC	428.91	393.1	396.53
Observations	104	104	104
R^2	0.068	0.369	0.376
Adjusted R^2	0.059	0.356	0.357
F Statistic	7.491^{***} (df = 1; 102)	29.484^{***} (df = 2; 101)	20.083^{***} (df = 3; 100)
Note:			*p<0.1; **p<0.05; ***p<0.01
	Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.		

Table 18. Proving the mediation of risk belief between age and behavioural intention in three steps.

	Dependent variable:		
	risk_belief	behavioural_intention	
	(1)	(2)	(3)
risk_belief			-1.003^{***} $(-1.130, -0.876)$
age	0.288^{**} $(0.068, 0.507)$	-0.366^{***} $(-0.629, -0.104)$	-0.078 $(-0.226, 0.071)$
Constant	-0.326 $(-0.899, 0.248)$	0.419 $(-0.267, 1.106)$	0.093 $(-0.285, 0.471)$
AIC	383.74	420.98	296.69
BIC	391.68	428.91	307.27
Observations	104	104	104
R^2	0.061	0.068	0.723
Adjusted R^2	0.052	0.059	0.718
F Statistic	6.614^{**} (df = 1; 102)	7.491^{***} (df = 1; 102)	132.067^{***} (df = 2; 101)

Note: $^{*}p<0.1$; $^{**}p<0.05$; $^{***}p<0.01$
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). (Gaussian) linear models.

7.5 Willingness to Pay for Non-Disclosure

Risk belief and age were hypothesized to have a direct effect on risk behavioural intention. Since one of the sub goals of this research is to establish if willingness to pay (WTP) behaves in the same way as behavioural intention, it makes sense to also investigate the effects of risk belief and age on WTP. Additionally the potential effect of protection belief on WTP is looked into.

The shape of the distribution of willingness to pay invites for General Linear Modeling for a negative binomial (see Figure 12). Testing out the different models for different distributions has showed a better fit for negative binomial versus Gaussian and Poisson distribution models, by means of smaller standard errors, AIC and deviance. Therefore General Linear Modeling was used to predict the variable WTP.

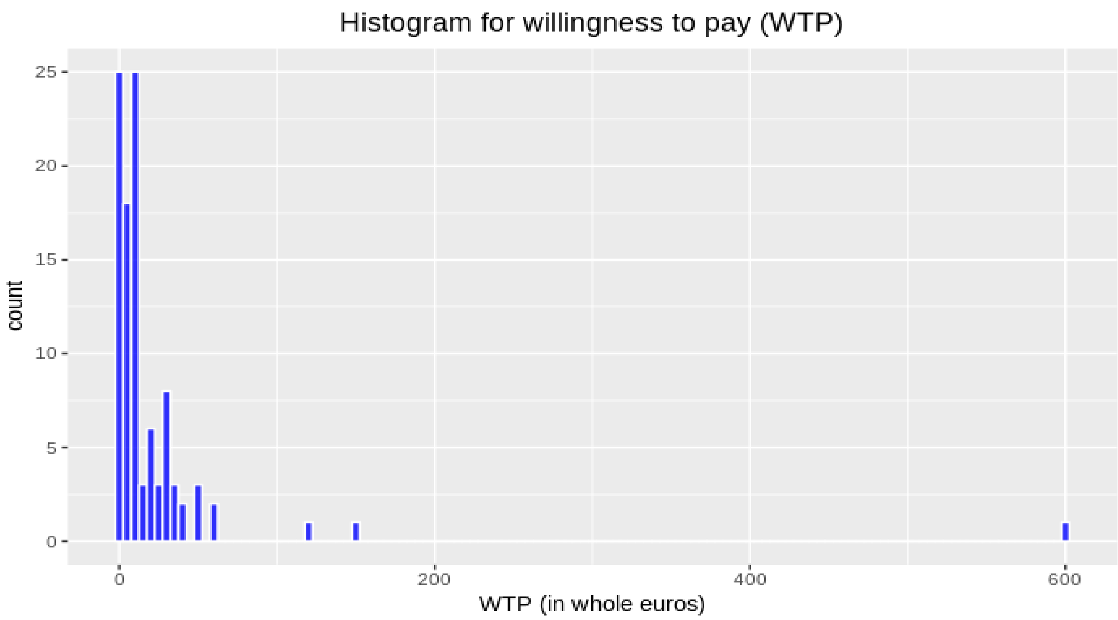

Fig. 12. Distribution of willingness to pay (WTP).

Risk Belief. There seems to be small positive effect of risk belief on willingness to pay of around 50 euro cents per additional point on the risk belief 7-point Likert-type scale. For high information sensitivity there seems to be a 10 euro cents more willingness to pay. However, testing the model with the interaction between risk belief and information sensitivity included, tells us that the interaction is not significant by means of its 95% confidence interval. Additionally, information sensitivity does not seem to have an effect on willingness to pay. Thus it seems that risk belief is no mediator between sensitivity and willingness to pay, while information sensitivity also does not affect willingness to pay directly (see Table 19). Still, risk belief positively affects willingness to pay. Therefore there can be hypothesized that there must be another latent variable affecting risk belief that makes the willingness to pay rise, or there is another variable at play that should be controlled for. A factor that could influence the relationship could be the income of the participant. From analysis the income seems not to have any practical or statistical effect on willingness to pay. The interaction between income and risk belief is however both of some practical and of statistical significance. For every 500 euros more in income, each extra point on the scale of risk belief seems to have about 8 euro cents more effect on the willingness to pay for non-disclosure (95% confidence interval between 2 euro cents and 15 euro cents). Risk belief cannot be said to mediate between income and willingness to pay, since the direct relationship of income to willingness to pay is insignificant (Dinev et al., 2013) (see Table 20).

Table 19. The effect of risk belief on willingness to pay and interaction with information sensitivity. Also the effect of only information sensitivity on willingness to pay.

	Dependent variable:			
	pay			
	(1)	(2)	(3)	(4)
risk_belief	0.407***	0.504***	0.528***	
	(0.227, 0.586)	(0.280, 0.728)	(0.231, 0.824)	
sensitivity		−0.611*	−0.544	0.030
		(−1.295, 0.074)	(−1.245, 0.158)	(−0.560, 0.619)
risk_belief:sensitivity			−0.097	
			(−0.549, 0.356)	
Constant	2.770***	3.041***	3.057***	3.046***
	(2.491, 3.048)	(2.611, 3.471)	(2.606, 3.508)	(2.611, 3.480)
AIC	775.09	773.51	775.35	792.02
BIC	782.94	783.97	788.42	799.86
Observations	101	101	101	101
Log Likelihood	−385.545	−383.757	−383.675	−394.008
θ	0.531*** (0.076)	0.550*** (0.079)	0.551*** (0.079)	0.451*** (0.062)

Note: $^{*}p<0.1$; $^{**}p<0.05$; $^{***}p<0.01$
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Models.

Table 20. The effect of risk belief on willingness to pay and interaction with income. Also the effect of only income on willingness to pay.

	Dependent variable:			
	pay			
	(1)	(2)	(3)	(4)
risk_belief	0.407***	0.331***	0.052	
	(0.227, 0.586)	(0.167, 0.495)	(−0.261, 0.364)	
income		−0.008	−0.075	0.054
		(−0.122, 0.106)	(−0.191, 0.040)	(−0.070, 0.177)
risk_belief:income			0.080**	
			(0.013, 0.146)	
Constant	2.770***	2.465***	2.651***	2.434***
	(2.491, 3.048)	(1.955, 2.975)	(2.149, 3.153)	(1.880, 2.988)
AIC	775.09	642.26	638.2	655.11
BIC	782.94	652.26	650.7	662.61
Observations	101	90	90	90
Log Likelihood	−385.545	−318.131	−315.100	−325.557
θ	0.531*** (0.076)	0.701*** (0.117)	0.756*** (0.128)	0.581*** (0.092)

Note: $^{*}p<0.1$; $^{**}p<0.05$; $^{***}p<0.01$
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Modeling.

Age. On first sight age seems to have a positive effect on willingness to pay of about 23 euro cents per about 10 years (one bin) over both information-sensitivity treatments combined. When splitting up the treatment groups it seems that only for the low information sensitivity effect is of practical and statistical significance with about 58 euro cents more per age bin. When adding the interaction to a model, then the interaction seems of high practical and of statistical significance (see Table 21).

In the low information-sensitivity treatment group the mean age was a little bit higher than in the high sensitivity group. Since age and income are highly correlated the influence of income could be further investigated. Looking into income affecting the effect between age and willingness to pay reveals that the interaction between income and age is non-significant (see Table 22).

Therefore we check if income might be a mediator between age and willingness to pay (see Table 23). Following the previously explained steps to determine mediation, we indeed found evidence that income is a mediator between age and willingness to pay. One of the prerequisites for this is that the effect of age on income needs to be significant, which it is. Using a negative binomial general linear model to approach the effect of age on income, tells us that on average for about each 40 years extra the spendable income would be 500 euros (one bin) higher.

Since age was already found to have an effect on risk belief, it makes sense to see if risk belief acts as a mediator between age and WTP. It appears that risk belief is also a mediator between age and willingness to pay (see Table 24).

Table 21. The effect of age on willingness to pay and interaction with information sensitivity.

	Dependent variable:		
	pay		
	(1)	(2)	(3)
age	0.233^{**}	0.261^{**}	0.582^{***}
	(0.009, 0.457)	(0.037, 0.485)	(0.279, 0.885)
sensitivity		0.186	1.347^{**}
		(−0.398, 0.769)	(0.205, 2.490)
age:sensitivity			-0.507^{**}
			(−0.951, −0.063)
Constant	2.517^{***}	2.351^{***}	1.566^{***}
	(1.943, 3.092)	(1.677, 3.025)	(0.743, 2.390)
AIC	789.34	790.99	790.06
BIC	797.18	801.45	803.13
Observations	101	101	101
Log Likelihood	−392.668	−392.493	−391.029
θ	0.462^{***} (0.064)	0.464^{***} (0.064)	0.476^{***} (0.066)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Modeling.

Table 22. The effect of age on willingness to pay and interaction with income.

	Dependent variable:		
	pay		
	(1)	(2)	(3)
age	0.233^{**}	−0.201	-0.501^{*}
	(0.009, 0.457)	(−0.498, 0.095)	(−1.086, 0.083)
income		0.121	−0.148
		(−0.042, 0.284)	(−0.461, 0.165)
age:income			0.085
			(−0.023, 0.193)
Constant	2.517^{***}	2.581^{***}	3.390^{***}
	(1.943, 3.092)	(1.994, 3.167)	(2.215, 4.564)
AIC	789.34	655.98	656.12
BIC	797.18	665.98	668.62
Observations	101	90	90
Log Likelihood	−392.668	−324.990	−324.061
θ	0.462^{***} (0.064)	0.589^{***} (0.094)	0.603^{***} (0.097)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Modeling.

Table 23. Mediation test for income as mediator between age and WTP.

	Dependent variable:		
	income	pay	
	(1)	(2)	(3)
age	0.257^{***}	0.233^{**}	-0.201
	(0.185, 0.329)	(0.009, 0.457)	(−0.498, 0.095)
income			0.121
			(−0.042, 0.284)
Constant	0.761^{***}	2.517^{***}	2.581^{***}
	(0.549, 0.974)	(1.943, 3.092)	(1.994, 3.167)
AIC	347.82	789.34	655.98
BIC	355.32	797.18	665.98
Observations	90	101	90
Log Likelihood	−171.912	−392.668	−324.990
θ	70,164.730 (1,247,987.000)	0.462^{***} (0.064)	0.589^{***} (0.094)

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Modeling.

Table 24. Mediation test for risk belief as mediator between age and WTP.

	Dependent variable:		
	risk_belief	pay	
	OLS	*negative binomial*	
	(1)	(2)	(3)
risk_belief			0.389^{***}
			(0.206, 0.573)
age	0.288^{**}	0.233^{**}	0.074
	(0.068, 0.507)	(0.009, 0.457)	(−0.141, 0.289)
Constant	−0.326	2.517^{***}	2.608^{***}
	(−0.899, 0.248)	(1.943, 3.092)	(2.067, 3.149)
AIC	383.74	789.34	776.82
BIC	391.68	797.18	787.28
Observations	104	101	101
R^2	0.061		
Adjusted R^2	0.052		
Log Likelihood		−392.668	−385.409
θ		0.462^{***} (0.064)	0.532^{***} (0.076)
F Statistic	6.614^{**} (df = 1; 102)		

Note: *p<0.1; **p<0.05; ***p<0.01
Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). OLS and Negative Binomial Generalized Linear Modeling.

Protection Belief. Contrary to the hypothesis, a small positive effect of protection belief on willingness to pay for non-disclosure seems to exist for both treatments combined and with a larger effect size for the low information sensitivity. It does not seem practically and statistically significant for the high information-sensitivity treatment group. When looking at the interaction between protection belief and sensitivity treatment, the interaction seems indeed to be quite substantial in its negative effect size and both practically and statistically significant. This would mean that people with a one point higher protection level (on a 7-point likert scale) would be willing to pay around 42 euro cents more when information sensitivity is low, but not when the sensitivity of the information at stake is high (see Table 25). This interaction is quite unusual, because the protection belief question is supposed to be independent of the treatment. The interaction could be caused by the place of the question in the questionnaire. It came near the end after the treatment had been administered in the form of the scenario. The kind of information might have been anchored in the minds of the participants, which would make them form their protection level with that information sensitivity still in mind. In that case, they would believe their protection level to be higher when having had the low information-sensitivity treatment, compared to the high information-sensitivity treatment. And that could have created the measured effect. From looking at the difference between the mean protection beliefs of low versus high sensitivity treatment groups (0.30; though not significant when taking into account its 95% confidence interval) it seems that this could be a plausible explanation for a large part of the interaction effect which was found.

Table 25. The effect of protection belief on willingness to pay and including interaction with information sensitivity.

	Dependent variable:		
	pay		
	(1)	(2)	(3)
protection	0.174^{*}	0.214^{**}	0.420^{***}
	(-0.005, 0.354)	(0.034, 0.394)	(0.175, 0.665)
sensitivity		0.353	0.291
		(-0.225, 0.931)	(-0.276, 0.857)
protection:sensitivity			-0.414^{**}
			(-0.765, -0.064)
Constant	3.049^{***}	2.852^{***}	2.787^{***}
	(2.759, 3.339)	(2.427, 3.278)	(2.372, 3.201)
AIC	787.56	788.38	784.21
BIC	795.41	798.84	797.29
Observations	101	101	101
Log Likelihood	-391.782	-391.191	-388.107
θ	0.470^{***} (0.065)	0.476^{***} (0.066)	0.505^{***} (0.071)
Akaike Inf. Crit.	787.564	788.381	784.214
Note:			*p<0.1; **p<0.05; ***p<0.01

Coefficients followed by 95% confidence intervals (calculated for normal/z-distribution). Negative Binomial Generalized Linear Modeling.