A BEHAVIOURAL PERSPECTIVE ON THE PRIVACY CALCULUS MODEL

Maria Moloney Valerio Potì[a]

Initial Draft: October 2013
This version: 13 April 2016

Abstract

This paper investigates how IS users make informational privacy-related decisions and how they manage their informational privacy risk. It puts forth a revised privacy calculus (RPC) model which allows for bounded rationality and ambiguity in explaining informational privacy decision making in the face of uncertainty. The model is tested using regression analysis of survey data and semi-structured interviews conducted with a sub-sample of the survey participants. The findings generally support the RPC model. In the face of ambiguity, both an individual's willingness to disclose personal information and his/her propensity to engage in privacy risk handling behaviour decrease, indicating that privacy risk handling behaviour takes place only in the presence of "quantifiable" uncertainty, to which we refer as risk, when trying to reduce it to an acceptable level. In the presence of ambiguity or "unquantifiable" uncertainty, risk handling behaviour is seen as pointless. A related important finding is that self-reported risk handling behaviour intensity is negatively impacted by the individual's propensity to trust, which acts as an ambiguity perception dampener.

Keywords: *Privacy, risk perception, trust propensity, behavioural intention, social contract, behavioural economics.*

Contact details:

[a] Contact author: Valerio Potì, Room Q233, University College Dublin, UCD Michael Smurfit School of Business, Carysfort Avenue, Blackrock, Co. Dublin, Ireland; Tel: 3531-7005823, Fax: 3531- 7005446; Email: valerio.poti@ucd.ie.

A BEHAVIOURAL PERSPECTIVE ON THE PRIVACY CALCULUS MODEL

Abstract

This paper investigates how IS users make informational privacy-related decisions and how they manage their informational privacy risk. It puts forth a revised privacy calculus (RPC) model which allows for bounded rationality and ambiguity in explaining informational privacy decision making in the face of uncertainty. The model is tested using regression analysis of survey data and semi-structured interviews conducted with a sub-sample of the survey participants. The findings generally support the RPC model. In the face of ambiguity, both an individual's willingness to disclose personal information and his/her propensity to engage in privacy risk handling behaviour decrease, indicating that privacy risk handling behaviour takes place only in the presence of "quantifiable" uncertainty, to which we refer as risk, when trying to reduce it to an acceptable level. In the presence of ambiguity or "unquantifiable" uncertainty, risk handling behaviour is seen as pointless. A related important finding is that self-reported risk handling behaviour intensity is negatively impacted by the individual's propensity to trust, which acts as an ambiguity perception dampener.

1. Introduction

Informational privacy is defined by Westin (2003) as *"the claim of an individual to determine what information about himself or herself should be known to others…This also involves when such information will be obtained and what uses will be made of it by others" (Westin, 2003, p431).* The decision to interact online in a manner that might put informational privacy at risk and the strategies that IS users deploy to handle such risk are instances of decisions made under conditions of uncertainty. In the IS literature, there is a common understanding that privacy decisions involve trade-offs between uncertain costs and benefits of personal information disclosure and the process through which IS users evaluate such trade-offs and make their privacy-related decisions has come to be known as the *Privacy Calculus* (Chellappa & Sin, 2005; Dinev, et al., 2006; Hann, et al., 2008). A number of models from previous IS privacy research that examine the privacy calculus have largely assumed that users behave rationally when evaluating privacy trade-offs

(Dinev, et al., 2006; Xu, et al., 2009). These traditional formulations of the privacy calculus (PC) model broadly postulate the IS users' ability to assess the risks and prospective benefits involved by the decisions they face, resulting in essentially informed and coherent goal-oriented decision making.

Acquisti and colleagues (Acquisti & Grossklags, 2005; Acquisti, 2009), challenge this view of privacy-related decision making. Their research uses a behavioural economics perspective and suggests that inconsistent behaviour by users regarding disclosure of personal information is the result of psychologically-motivated distortions to their preferences (e.g., hyperbolic discounting of risks), limited or asymmetric information, and bounded rationality. They argue that it is because of these limitations that users have the tendency to supply private information in return for relatively small conveniences or rewards, even when their stated informational privacy concerns do not support this behaviour, a set of circumstances that has become known as the *privacy paradox* (Wilson & Valacich, 2012).

As noted by Acquisti and Grossklags (2008), the economics literature has devoted considerable effort, over many decades, to the study of the problem of decision making under uncertainty yet, due to limited interaction between researchers in IS and economists, the understanding of decision making in the IS domain has not yet fully benefited from such efforts. Following the literature on limits to rationality and insights from the behavioural economics literature, we conceptualize individuals as possibly imperfectly rational decision makers, in the sense of being either imperfectly informed or imperfectly able to process information (or both), who are subject to bias and error (Shefrin, 2002; Acquisti and Grossklags, 2008) and may face, or at least perceive, ambiguity (Knightian uncertainty) when making decisions concerning their

online privacy. This leads us to put forth a *Revised* Privacy Calculus (RPC) Model, which is the PC model augmented by insights from behavioural economics and psychology.

Ultimately, this study seeks to understand if an individual's decision to disclose his/her personal information online in the presence of quantifiable uncertainty is different from the decision that occurs in the presence of unquantifiable uncertainty or ambiguity, while admitting cognitive error and/or bias in the assessment of privacy risk. To test the RPC model, we first conduct a survey and analyse the results based on multivariate regression analysis. Semi-structured interviews with a subsample of the survey participants were then conducted two months after the questionnaire was completed. They were carried out to better capture constructs that were weakly measured by the questionnaire and to shed light on implications of the RPC model that remained unclear after the regression analysis of the results.

In what follows, we review, in section 2, the contributions made by the economics literature to the understanding of decision making under uncertainty. We then review, in section 3, the literature on IS users' decisions in the face of online privacy risk, with special emphasis on the privacy calculus (PC) model (Dinev, et al., 2006). In section 4, we extend the PC Model to account for the possible influence of heuristic driven cognitive biases, along the lines of the seminal work of Kahneman and Tversky (1979), and ambiguity (Acquisti & Grossklags, 2005), leading to a revised privacy calculus (RPC) model. We then show, in section 5, the results of tests carried out on the RPC model using first regression analysis of survey data and then data from the semi-structured interviews. Finally, in the last section, we offer our conclusions and outline avenues for future research.

2. Decision Making Under Uncertainty

There are at least two broad paradigms in the economics literature with respect to goal-driven decision making under uncertainty. One such paradigm, which includes theories of '*rational decision making*', assumes that the decision-maker is both fully rational, in the sense of being able to make coherent choices among all available alternatives, and is endowed with a large amount of information. The other paradigm, which includes theories of '*imperfectly rational decision making*', allows for less than full rationality on the part of the decision makers, and/or limited information available to them. It consisted initially of theories based on '*bounded rationality*' (Simon, 1957) and later it broadened into the *behavioural economics* critique of the rational decision making paradigm (Kahneman & Tversky, 1979). A further perspective, sometimes intertwined with either the bounded rationality or the behavioural perspective, is that which emphasises ambiguity or "Knightian Uncertainty." We shall briefly review each of these perspectives.

2.1 Rational Decision Making

A crucial role in models of rational decision making under uncertainty is played by Expected Utility Theory (EUT), originally formulated by von Neumann and Morgenstern (1947). In EUT, decision-makers use a well-defined mathematical object known as a utility function to rank alternatives and make coherent decisions. EUT also assumes that decision-makers have enough information to adopt such a structured approach to decision making, which entails considerable 'computational' requirements (Anand, 2002). This is the assumption made by the rational expectation (RE) hypothesis (Muth, 1961). This hypothesis implies that the weights assigned to

possible outcomes in calculating expected utility, i.e. the decision making goal under EUT, correspond to the true probability of such outcomes.

2.2 Bounded Rationality

A second paradigm revolves around the concept of 'bounded rationality.' It assumes that, in the presence of limited information and/or limited information processing capacity on the part of the decision maker, the latter either replaces expected utility maximization or complements it with other less demanding decision making rules, for example heuristics and rules based on adaptive learning. The paradigm follows the seminal work of Simon (1957), who assumes that actors are goal-oriented, but it also considers the cognitive limitations of decision makers in attempting to achieve those goals.

Psychologists Kahneman and Tversky (1972) laid the foundations for a comprehensive reappraisal of decision making under uncertainty within the economics literature. They described three general-purpose heuristics, "*availability*", "*representativeness*" and "*anchoring and adjustment*," that underlie many intuitive judgments under uncertainty. These heuristics, they suggested, are simple and efficient because they piggyback on basic cognitive computations (Gilowich et al. 2002).[1] *Representativeness* is "the degree to which [an event] 1) is similar in essential characteristics to its parent population, and 2) reflects the salient features of the process by which it is generated" (Kahneman and Tversky, 1972, p. 431). When used

[1] For instance, many people rely on media for information about deaths by homicide. If the media reports type A cause of death more than type B, people who rely on *availability* heuristics believe the former to be the main cause of death between the two causes because, due to the media reporting, they recall instances related to type A more readily than type B. The availability of information about type A cause of death leads them to conclude it is the main cause of death. Thus media coverage biases a rule based on recall (Shefrin, 2002).

to form the basis for judgement, it gives rise to a cognitive bias to the extent that an individual categorizes a situation based on a pattern of previous experiences or consolidated beliefs about that situation, rather than on the basis of rationally (according to Bayesian learning) updated beliefs.[2] The *anchoring* bias emerges when individuals need to reach some judgment. Initially they form a preliminary judgment from some simple feature (anchor) and then adjust this estimate to form a final judgment. The adjustment, however, is usually conservative (relative to a rational benchmark given by Bayesian updating of beliefs), and hence the final judgment is usually biased towards the initial anchor[3]. These heuristics can be seen as learning rules developed by humans to deal with limits to their own rationality or with the incompleteness of the information set. The behavioural economics literature sees these as biased and, ultimately, at least partially inconsistent, albeit efficient, rules. An emerging strand of the bounded rationality literature, e.g. Gigerenzer & Selten (2002), admit instead that such rules can be unbiased or at least consistent, as well as efficient, and lead to essentially rational decision making even in the presence of limits to rationality.

2.3 Knightian Uncertainty

Knight (1921) proposed to distinguish situations characterized by risk, in which the possible random outcomes of a certain event have known associated probabilities,

[2] The simplest example of using such a principle in forming beliefs is to predict that university GPA will be the same as high school GPA. Thus, a student with a high GPA in school is seen as representative of a good student. This does not necessarily predict their performance at university (Shefrin, 2002), as it is not based on knowledge of the causal model of university performance.

[3] Thus, if an individual primarily perceives (or anchors) an online entity to be risky, for any number of reasons, then the final judgement (adjustment) is likely to be biased toward the initial anchor and hence towards the initial assessment that the entity is risky, even after additional information suggests otherwise.

from those characterized by uncertainty or ambiguity, in which the randomness cannot be expressed in terms of mathematical probabilities, and the probabilities themselves are unknown or unknowable. The latter type of uncertainty has come to be known as *ambiguity* or Knightian uncertainty. In decision theory and economics, ambiguity aversion, also known as (Knightian) uncertainty aversion, plays an important role in models of decision making under uncertainty. There is evidence that decision makers frequently exhibit ambiguity aversion (Erbas & Mirakhor, 2007), also known as (Knightian) uncertainty aversion.[4] Shefrin (2002) argues that the aversion to ambiguity is due to fear of the unknown but, unlike the heuristic biases, it is not a cognitive error, at least to the extent that the perceived ambiguity corresponds to true ambiguity and is not itself a biased judgement.

3. Privacy as a Commodity and the Privacy Calculus

Value-based definitions of privacy argue that a call for greater privacy is, fundamentally, antagonistic to the political economy of the information markets (Posner, 1978; Lessig, 2000; Cohen, 2001). In this view, privacy is not an absolute right but is subject to the economic principles of cost–benefit analysis and trade-offs. This view has originated a stream of research regarding privacy as a commodity (Davis, 2010; Johnston, 2012). From this perspective, privacy is still seen as an individual and societal value, but it is no longer an absolute. It can be assigned a negotiable economic value and can be considered in a cost-benefit calculation at both individual and societal

[4] When ambiguous prospects are presented to users alongside risky but unambiguously defined prospects, users often opt for the latter, choosing the option with fewer unknown elements than the option with many unknown elements. For example, individuals prefer to bet on a bag with 50 red and 50 blue poker chips than on one with 100 total poker chips but where the number of blue or red chips is unknown.

levels. This calculation, which has become known as the *privacy calculus* (PC), involves weighing the perceived costs against the perceived benefits of the transaction, with disclosure the result of a rational choice when benefits outweigh costs (Wilson & Valacich, 2012).

The informational privacy and sociology literature conceptualizes the PC by assuming individuals carry out a trade-off calculation based on costs and benefits when determining their course of action. This perspective is found in various sociological and legal studies (e.g., Klopfer and Rubenstein 1977; Posner 1981; Stone and Stone 1990). For example, as put by Stone and Stone (1990, p. 363), "*individuals are assumed to behave in ways that they believe will result in the most favourable net level of outcomes*". This literature (often somewhat implicitly) assumes individuals, in the presence of uncertainty in privacy-related decisions, weigh outcomes by their likelihood and the cost-benefit trade-off becomes a trade-off between some definition of risk[5] and (expected) reward, with the latter defined as the benefit from the transaction net of costs not already included in the definition of risk. More recent literature on the PC more explicitly suggests that, when requested to provide personal information, individuals perform a risk–reward analysis to assess the outcomes of the disclosure, and respond accordingly (Hui, et al., 2007; Smith, et al., 2011). For example, Consumers make trade-offs between the conveniences of "free" personalization services offered by many websites and the breach of privacy that results in sharing preference information required to use these personalization

[5] An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences (Peter and Tarpey, 1975). The negative perceptions related to risk may affect an individual emotionally, materially, and physically (Moon, 2000).

services (Chellappa & Shivendu, 2010). An important aspect of online personalization is that these services are generally offered free of charge. However, consumers may not use all offered services even if they value personalization, as they are likely to be concerned about the privacy of the information that they share in order to use these services. Such privacy concerns are indeed valid because the business rationale behind free services is often based on the exploitation of consumers' preference information, such as for pricing and targeted advertising (Chellappa & Shivendu, 2007). Conversely, Arona, et al. (2006) argue that a number of online companies willingly do not (over) use or sell their customers' preference information because, unless the online companies commit to this 'reduced usage' guarantee, their customers will not provide the information at all. Similarly, Hann et al (2008) found that, when sellers market goods to consumers through solicitation, consumers often employ methods of concealment or deflection to avoid such marketing efforts and reduce the likelihood of being solicited.

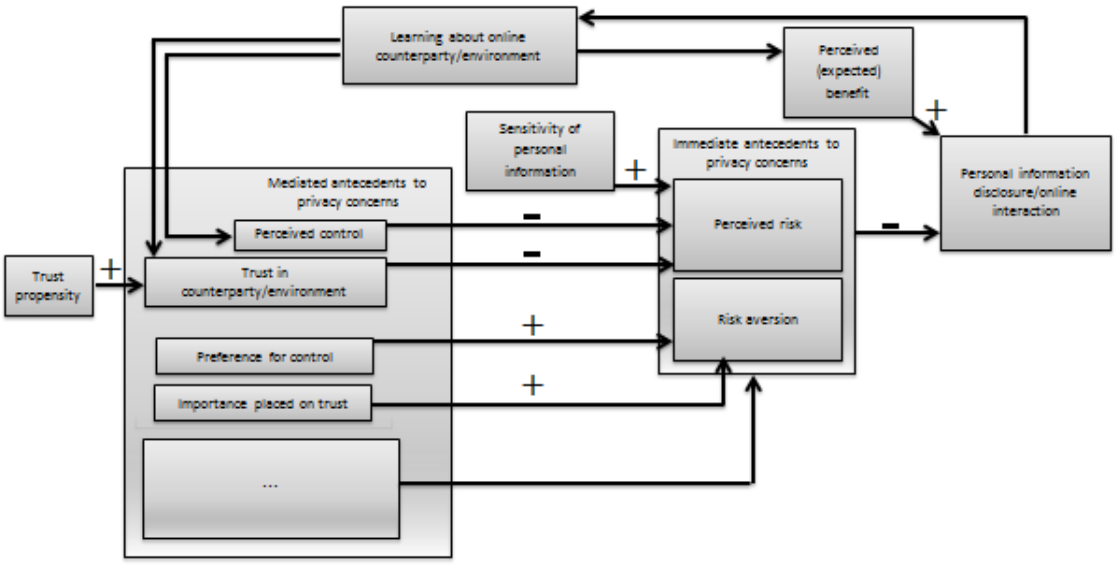
Given the specific definition of risk and benefits adopted by a given instance of the PC model, it is possible to interpret the model itself as a specialized version of models of decision-making under uncertainty prevalent within the rational paradigm reviewed in the previous section. Figure 1 summarizes the main constructs, and relations thereof, that characterize typical formulations of the PC model, consistent with a rational assessment of the trade-off between risk and reward.

Compared to the traditional representation of the PC typically found in IS studies, the one in the Figure makes more direct use of key constructs from the theory of rational decision making under uncertainty, namely perceived risk and risk aversion. Instead of directly linking privacy concerns to the decision of whether to disclose personal

information, it emphasizes the effect of perceived risk and risk aversion on the latter, interpreting traditional privacy concerns as antecedents to these two key constructs.[6] The advantage of this representation is that it highlights the different roles of perceived risk and risk aversion. This is useful because perceived risk depends on the situation at hand, whereas risk aversion is a depiction of individuals' attitudes that are thought to be, at least in the short run, invariant to the specific circumstances of the interaction. The Figure also shows that trust depends on propensity to trust, which can be seen as a mediated antecedent to trust, risk perception and privacy concern. In the representation of the PC depicted in Figure 1, the individual forms beliefs about the benefits of the transaction as well as concerns about privacy, which are functions of both the perceived riskiness of the transaction and of the individual's attitudes towards risk (summarized by his/her risk aversion), based on available information acquired through learning about the online environment and counterparty. We refer to perceived risk and risk aversion as immediate antecedents to privacy concerns and label other antecedents as mediated antecedents to privacy concerns.

Figure 1
The Privacy Calculus Model (PC)

[6] The flowchart in the figure shows that an individual uses available information to form his/her perception of the benefits and of the riskiness of the interaction in question, having firstly formed a perception of the control exerted over his/her personal information and of the trustworthiness of the counterparty. The decision whether to disclose personal information to interact online then depends on the individual's risk aversion, which in turn depends on the individual's preference for control and importance placed on trust, as well as on the sensitivity of the information that needs to be shared to interact online.



4. The Revised Privacy Calculus (RPC) Model

In this section, we put forth a revised privacy calculus (RPC) model which allows for bounded rationality in informational privacy decision making in the face of uncertainty, including ambiguity.[7] We allow for two qualitatively different types of limits to rationality:

1. Cognitive error in the assignment of probabilities to possible outcomes, possibly due to the use of bias-prone heuristics, leading to a systematically[8] wrong assessment of the risk-reward trade-off of online risky prospects;

[7] As before, we interpret online interactions as transactions that involve some uncertain prospect of threat to privacy and some attendant loss that may be suffered by an individual following the release of personal information to an external entity (e.g., an organization or another individual). Here, loss is defined broadly as any undesired outcome (resulting from the disclosure of personal information).

[8] The circumstance that the error may be systematic is important as it implies that it cannot be dismissed as being, on average, irrelevant.

2. Inability to assign probabilities to all possible outcomes, which may result in (subjective) ambiguity or perception thereof.

It is worth noting that, with regard to the second of the two limits to rationality listed above, a *subjective* rather than *objective* notion of ambiguity (or Knightian uncertainty) enters the definition. That is to say, unlike in the standard definition of ambiguity, we do not require it to be impossible to assign probabilities to outcomes, but simply that the particular decision maker under consideration is not able to do so, or at least perceives an inability to do so. This subjective definition of ambiguity is relevant to information disclosure in an online and ICT-mediated setting because the typical IS user often does not know how to assess the risk that another entity gains access to or uses his/her personal information once it is submitted online (Varian, 1997), whereas an experienced and IS-savvy user might know how to do this. It is, by definition, impossible to quantify ambiguity. Nonetheless, decision makers would perceive it in settings in which they felt aware of their own inability to assign probabilities to outcomes of interest.[9] In such circumstances, subjectively defined ambiguity would have the same implications for decision making as objective ambiguity.

Accordingly, we interpret decision-making concerning disclosure of personal information as an instance of decision-making under different degrees of uncertainty and, in accordance with Shefrin (2002), we classify uncertain events that may occur in online and IS-mediated interactions in two categories: risky and ambiguous events.

[9] An individual's calculation of risk involves an assessment of the probabilities of negative consequences occurring as well as the perceived severity of those consequences once they occur (Peter & Tarpey, 1975).

Risky events are those for which individuals can assign a known/knowable probability to each possible outcome. Ambiguous events are those for which such assignment is impossible, either because the probabilities are unknown/unknowable or because one or more possible outcomes are not known/knowable, and therefore are characterized by a qualitatively different type of uncertainty. That is, the term risk is reserved in this research to denote situations characterized by *quantifiable* uncertainty whereas ambiguity is used to refer to situations characterized by *unquantifiable* uncertainty, namely uncertainty of the Knightian sort.

We assume that, when *limits to rationality* are *not binding*, IS users make decisions by choosing the course of action that maximizes the expectation of a well-defined utility function, just like under the rational decision making paradigm. Unlike under this paradigm but consistent with the behavioural economics perspective, however, we allow for the possibility that *limits to rationality* are *binding*, either to an extent that leads the IS user to resort to heuristic decision making rules (to 'save on scarce rationality') or to an extent that leads the user to perceive the situation as *ambiguous*. Following the behavioural literature, and especially Shefrin (2002), we allow for the possibility of systematic error in assigning probabilities to outcomes when the user is subject to limits to rationality and resorts to heuristics, while not ruling out that, as proposed by Gigerenzer & Selten (2002), reliance on heuristics may result in essentially rational decision making[10]. Following the literature on Knightian

[10] Kahneman and Tversky (1972) suggest that individuals resort to bias-prone heuristics, or rules of thumb, to cope with their limits to rationality. In contrast, Gilowich et al. (2002), note that using "common sense" generally does work to make sense of the world, advocate adaptive behaviour and remark that, in general, causes resemble effects and appearances are usually good indicators of reality.

uncertainty/ambiguity, we posit that the user disengages when he/she perceives ambiguity.

Consistent with the IS literature on the PC, this implies that the IS user evaluates a certain risk-reward trade-off, based on certain risk preferences (though this is not usually made explicit in the PC literature), and a certain way to combine preferences with an assessment of the probabilities of outcomes, e.g. the expectation of the utility function or a mechanism with a similar effect (e.g., the expectation over the 'weighted' gains and losses considered by Kahneman and Tversky (1979)). We assume this to result in a ranking of choices concerning online behaviour that is a positive function of the expected benefit and a negative function of risk. As it is often the case in the PC literature, preferences are not specified any further.

In accordance with this approach, we define privacy risk as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity (Malhotra, et al., 2004). This definition of privacy risk is not derived from an explicit characterization of the decision maker's preferences, as the preferences are not fully specified, but it represents a widely adopted definition in the IS literature. It should be in principle possible to find a specification of preferences, e.g. a particular utility function, which implies this definition of privacy risk. Identifying such specification, however, is outside the scope of the present study though we note that it would represent a worthwhile endeavour for future research.

We also follow the prevailing literature on the PC in defining the reward element of the risk-reward trade-off evaluated by the user. We assume the possible reward to consist of a certain combination of the three main types of benefits of information disclosure, i.e. financial rewards, personalization, and social adjustment benefits

(Smith, et al., 2011). It is worth noting that the fact that the trade-off evaluated by the IS user is a function of financial rewards is coherent with the PC model's tenet that privacy is, to some extent, negotiable, as well as with empirical evidence that compensating consumers through financial rewards encourages information disclosure (Hann, et al., 2008; Xu, et al., 2010).

To complete the model, we allow for the circumstance that the decision to disclose and interact online may be mediated by some *risk handling behaviour*. That is, the individual may decide to undertake risk handling behaviour before deciding to interact, based on his/her own assessment of the expected benefit and risk of the perspective interaction as well as his/her attitudes towards risk and propensity to trust. To model the risk handling decision, we make the assumption that risk handling behaviour is *costly*, e.g. in terms of administrative costs, delays, missed opportunity to interact, fees for specialized software, etc. The implications is that, for a given level of risk aversion, the rational choice for the individual is to undertake risk handling behaviour only if the expected benefit, net of risk handling behaviour costs, is large enough to compensate for the perceived risk of the interaction. Since risk handling behaviour itself has the potential to reduce risk and hence the perception thereof, the net effect is that the intensity of the risk handling behaviour undertaken in a given set of circumstances increases in the magnitude of both the perceived risk and expected benefit of the interaction.

Figure 2 overleaf summarizes the main constructs, and relations thereof, of the RPC model. Panel A of the figure focuses on the implications of the model for information disclosure. It is shown that the individual uses available information, acquired through learning about the online counterparty and environment, to form his/her perception

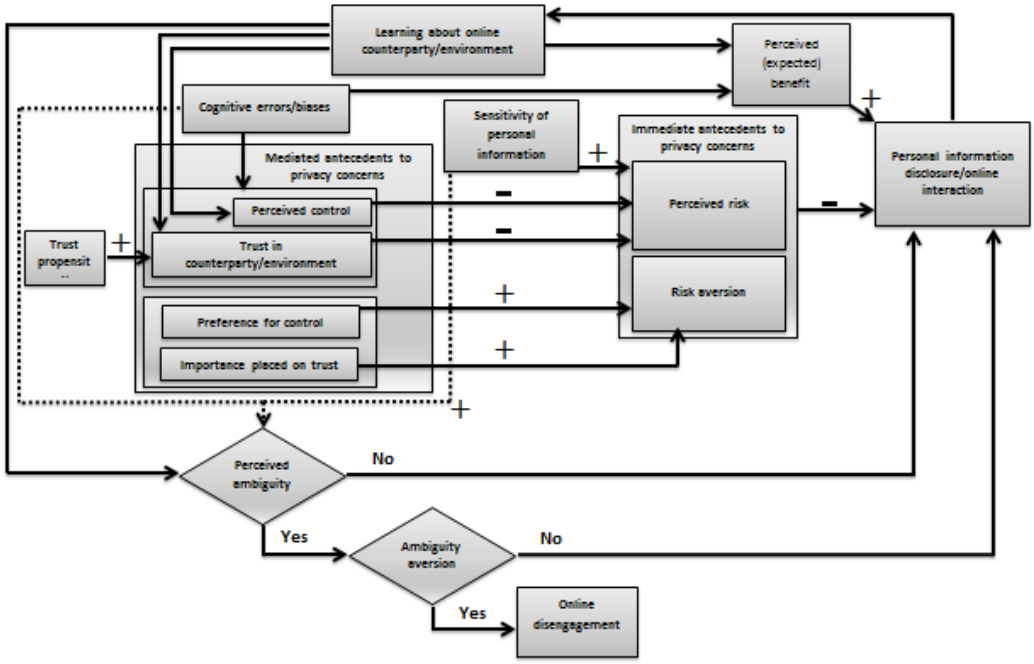
of the benefits and of the riskiness of the interaction in question, having formed a perception of the control exerted over his/her personal information and of the trustworthiness of the counterparty. Panel B generalizes Panel A, depicting the possible role of risk handling behaviour in privacy-related decisions and its joint determination alongside information disclosure. In contrast with the restricted version of the model (i.e., the traditional PC model) depicted in Figure 1, Panel B emphasises that, in the event that the individual perceives ambiguity and he/she is adverse to it, he/she will disengage rather than undertake risk handling behaviour.[11]

In Table 1, we put forth a number of hypotheses consistent with implications of the traditional (rational choice-based) and revised formulations of the PC model, corresponding to the visual representation of each model depicted in Panel A and B, respectively, of Figure 2. The hypotheses are labelled from H1 to H8, in the first column, and are described in the second one. In the third column, for each hypothesis, we specify further implications, where relevant. By way of comparison of the traditional and revised formulations of the PC model, we note in the last column that H1, H2, H5 and H6 are in common to both formulations (even though previous literature on the PC has placed more emphasis on explicitly modelling implications for information disclosure rather than for risk handling behaviour, and therefore H5 have received relatively little attention), whereas H3, H4, H7 and H8 hold only in the context of the RPC model.

[11] In this respect, it is conceivable that the perception of ambiguity is enhanced when the personal information that the individual is required to submit is highly sensitive. Accordingly, we include dotted arrows to allow for a positive effect of the sensitivity of personal information on perceived ambiguity.

Figure 2
The Revised Privacy Calculus (RPC) Model

Panel A



Panel B

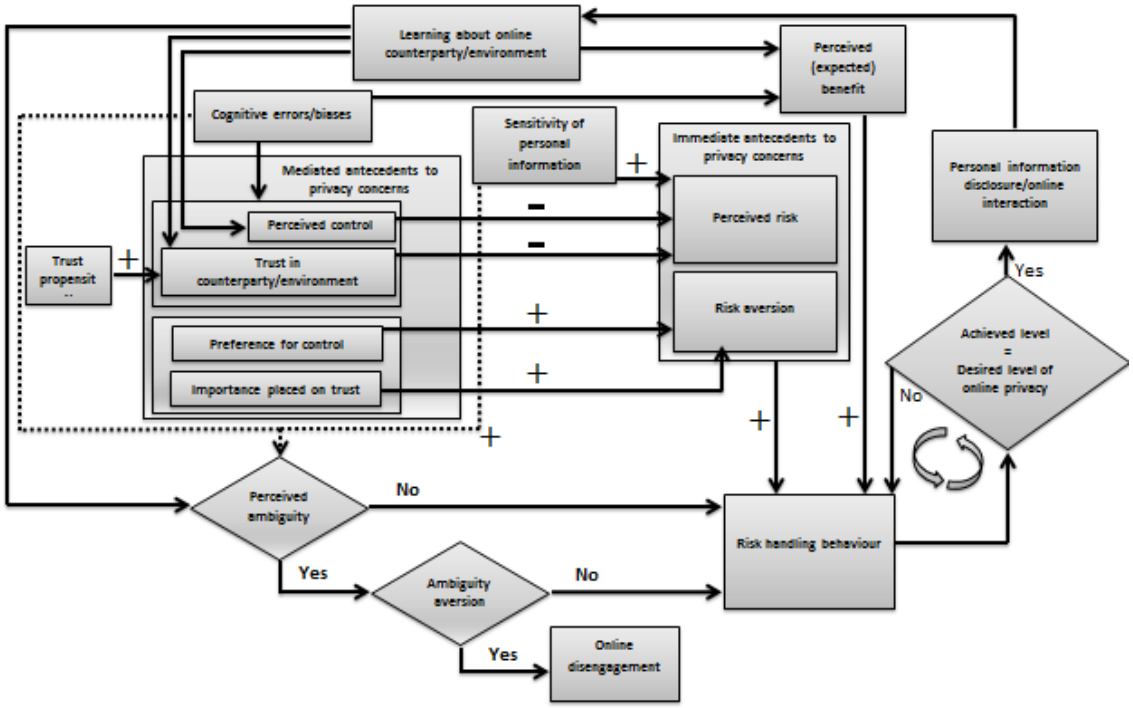


Table 1

Hypothesis	Description	Sub-hypotheses / implications		Consistent with PC model?
On the individual's **willingness to disclose personal information (Panel A)**				
H1	It is positively influenced by the perceived benefit of online interaction	It is positively impacted by the perceived *benefit* of disclosing personal information online, net of the expected *costs* of risk handling measures		Yes
H2	It is negatively influenced by *perceived risk*, for a given level of *risk aversion*, and *vice versa*	(a)	It is positively (negatively) influenced by negative (positive) antecedents of perceived risk such as (lack of) *perceived control* and (lack of) *trust* in the counterparty/online situation, for a given level of *risk aversion*	Yes
		(b)	It is negatively influenced by *preference for control* and by *importance placed on trust*, as antecedents of risk aversion, for given levels of *trust* in the counterparty/online situation and *propensity to trust*, respectively	Yes
H3	It is negatively influenced by *ambiguity*, for a given level of *ambiguity aversion*, and *vice-versa*	(a)	It is negatively impacted by *perceived ambiguity* and possible positive antecedents thereof, such as *age*	**No**
		(b)	It is negatively impacted the individual's *ambiguity aversion*, and possible positive antecedents thereof, such as *age*	**No**
H4	It is negatively impacted by *availability bias* when limits to rationality are binding	It is negatively impacted by the *recent occurrence of a privacy breach*.		**No**
On the individual's intensity of **risk handling behaviour (Panel B)**				
H5	It is positively impacted by the expected net benefit of the online interaction	It is positively impacted by the perceived *benefit* of disclosing personal information online, net of the expected *costs* of risk handling measures		Yes
H6	It is positively impacted by *perceived risk*, for a given level of *risk aversion*, and *vice-versa*	(a)	It is negatively impacted by negative antecedents of *perceived risk*, such as *perceived control* and *trust*, for given *propensity to trust* in online situations	Yes
		(b)	It is positively impacted by positive antecedents of *risk aversion*, including *preference for control* and *importance placed on trust*, and negatively by negative antecedents thereof, such as *propensity to trust*, for given *perceived control*	Yes
H7	It is negatively influenced by *ambiguity*, for a given level of *ambiguity aversion*, and *vice-versa*	(a)	It is negatively impacted by *perceived ambiguity* and possible positive antecedents thereof, such as *age*	**No**
		(b)	It is negatively impacted the individual's *ambiguity aversion*, and possible positive antecedents thereof, such as *age*	**No**
		(c)	It is positively impacted by the level of familiarity with IS and its positive antecedents, including *owning a compute*, *working in the computer industry* and *training and education*	**No**
H8	It is positively impacted by *availability bias* when limits to rationality are binding	It is positively impacted by the *recent occurrence of a privacy breach*.		**No**

5. The Survey: the Questionnaire and Semi-Structured Interviews

The first step of the survey was a questionnaire, followed by a regression analysis of the findings and semi-structured interviews. The next subsections explain how the data gathered from the questionnaire is analysed, how this data and multiple linear regression are used to test implications of extant theories of privacy and especially of our RPC model, and the results of this analysis. We then describe and analyse the semi-structured interviews.

5.1The Distribution of the Online Questionnaire

The target population for the online questionnaire were *adult online users*. To form a sample as wide and as representative as possible of the target population, we break down the latter by age groups, as consistent evidence shows that attitudes to online privacy vary considerably with age (Forrester Research, 2010). Five age groups were surveyed. These were 18 years and under; 18 years – 24 years; 25 years – 35 years; 36 years – 50 years; and 50 years and over.

Respondents in the first two groups (Under 18 and 18-24) were largely represented by undergraduate and post graduate students from Trinity College Dublin. The third and fourth groups of participants (25-35 and 36-50) were generally employees of the same university. Finally, the last group of users were largely represented by members from two local Rotarian clubs and were from the ages of 50 and upwards. In all, the questionnaire was sent out to 2500 individuals. There were 420 responses to the questionnaire, a response rate of a little under 17%. In the resulting sample of individuals from the young age groups, lower levels of education are not represented but the sample hopefully contains enough diversity in educational attainment (i.e., undertaking an under/postgraduate degree or having an under- and/or postgraduate

degree) so as to allow, in the subsequent regression analysis, the identification of the effect of education. Similar considerations apply to the sample of individuals in the older age groups, whose education levels are even more diverse, but with the caveat that there is limited variation in their socio-economic circumstances.

Overall, though this is, admittedly, an imperfect sampling scheme, likely to introduce some biases in the sample, we strived to mitigate their impact of this problem on our inferences by taking it into account in the subsequent multivariate regression analysis of the questionnaire results. We did this by including in the regression model and the semi-structured interviews a number of control variables corresponding to characteristics by which it would have been ideal (albeit impossible, given our resources) to stratify the sample.

From the questionnaire, we sought to sample proxy measures for nine constructs, i.e. (1) willingness to disclose personal information (*Willingness*), (2) perceived benefit from doing so (*PerBen*), (3) perceived risk (*PerRis*) in doing so, (4) propensity to trust (*PropTru*), (5) importance placed on trust (*ImpTru*), (6) control preference (*ContPref*), (7) ambiguity aversion (*AmbAver*), (8) availability bias (*Avail*) and (9) extent of (or propensity to engage in) risk handling behaviour (*RiskHand*). The final set of questions in the online questionnaire is set out in Appendix 1. The questions on constructs (1) to (8) are based on questions from the literature and adapted for this study, whereas the questions on construct (9) are, to the best of our knowledge, novel. This list of constructs includes all the constructs appearing in the RPC model (Figure 2), except the more situation-specific ones, such as the degree of *perceived control*, the *trust* in the online counterparty or the sensitivity of the personal information

required for the interaction, which are impossible to sample using standard survey methods.

In the survey, we only attempt to capture variation of attitudes and self-reported behaviour across subjects rather than variation of behaviour (per subject) across circumstances. Smith et al. (2011) acknowledge that this is a common limitation of empirical studies in the literature on informational privacy, which we seek to address by carrying out semi-structured interviews. In terms of our hypothesis, this means that, through our survey, we cannot test H2.(a), H3.(a), H6.(a) and H7.(a).

5.2 Regression Analysis of Questionnaire Results

We use a multiple linear regression framework, specified as a generalized linear model (GLM), to estimate the relations between the constructs sampled through the questionnaire, test the hypotheses previously listed (i.e., H1 to H8) and, this way, test the RPC against the more traditional formulation of the PC model. To identify the RPC model, our estimation methodology follows the "*general-to-specific*" approach, along the lines of Campos, Ericsson and Hendry (2005). We start with the most general regression model that includes, on the right hand side, the variables typically considered by the literature as well those suggested by our RPC model and we then eliminate regressors that appear not to explain the dependent variable, i.e. that carry statistically insignificant regression coefficients. Both the equations that, for each dependent variable, include all explanatory variables and those that, as a result of the general-to-specific variable selection procedure contain only a subset thereof, are to be seen as reduced-form representations of the corresponding structural models, which are left unidentified. As implied by Panel B of Figure 2, their identification would require the estimation of the joint determination of $Willingness_i$ and

$RiskHand_i$, a task that we leave for future research as it would require hard to obtain data on actual risk-handling behaviour choices and information disclosure decisions. The most general version of the reduced form regression model for either dependent variable, where dep_i denotes either $Willingness_i$ or $RiskHand_i$, is the following:

$$dep_i = Const. + \beta_1 ContrPref_i + \beta_2 AmbAver_i + \beta_3 PerRis_i + \beta_4 PerBen_i + \beta_5 PropTru_i + \beta_6 ImpTru_i + \beta_7 Avail_i + \beta_8 Age_i + \beta_9 Gender_i + \beta_{10} Education_i + \beta_{11} Home_{Comp_i} + \beta_{12} Work_{Comp_i} + \beta_{13} Comp_{Ind_i} + u_i \quad (1)$$

Here, the explanatory variables are denoted as in Tables 5-7 in Appendix and u_i denotes a regression error term. The estimates of this model are reported in Tables 2 and 3, for dep_i equal to $Willingness_i$ and $RiskHand_i$, respectively. For each model, we report point parameter estimates together with robust heteroskedasticity-adjusted standard errors and associated p-values under the null that the corresponding coefficient is equal to zero. We eventually settle on the models in the last lines of Table 2 and Table 3 for $Willingness_i$ and $RiskHand_i$, respectively (where, apart from the constant, we only leave variables that are significant at the 15 percent level). For comparison, each Table also reports the estimates of the restricted regression implied by the traditional PC model. In specifying the latter, we adopted a broad definition thereof, including among the regressors not only $PerBen$ and $PerRis$ but also variables that can be deemed to be related to privacy concern antecedents considered by the prior PC literature, namely $PropTru$, $ImpTru$ and $ContrPref$. In one of the two specifications of the PC model we consider, we also included Age and $Gender$ to control for un-modelled demographic influences, though it can be argued that both are related to demographic and socio-economic circumstances that might be correlated to limits to rationality and ambiguity aversion.

5.2.1 Model for willingness to disclose personal information

Regarding the RPC reduced-form model for *Willingness*, the final specification includes all variables except (the proxy) for informational privacy control preference, *ContrPref*, and the dummies for the occurrence of a recent privacy breach, *Avail*, and for whether the subject works in the computer industry, *ContrPref* and *Comp_ind*, that are excluded because their coefficients are not statistically significant. All other variables enter the regression with an estimated sign consistent with our RPC model[12], as can be seen by comparing the hypotheses in Table 1 with the estimates in Table 2. In particular, because of the estimated coefficients of $AmbAver_i$, Age_i (a proxy for *limits to rationality* with respect to the use of IS and possibly for *ambiguity aversion*), $Home_{Comp_i}$ and (at a more marginal level) $Work_{Comp_i}$, our results represent evidence against the more restricted traditional version of the PC model in favour of our (behaviourally-augmented) RPC model.

Surprisingly, the estimated coefficient of *ContrPref*, a variable that we are using as a proxy for *risk aversion*, is not negative (in fact, it is positive and insignificant). While this might be due to measurement error (an error in variable problem)[13], the fact that it is not statistically significant also suggests that there might not be enough variation in the values taken by this variable across the individuals in our sample to allow for an accurate estimate. In the semi-structured interviews, on which we shall report later,

[12] The fact that willingness to disclose personal information is positively related to the perceived benefit of the interaction is consistent with findings reported by Dinev and Hart (2004) and Malhotra et al. (2004) to name just two, as well as with our calculus model. Its negative relation with risk perception was already detected by Fetherman and Pavlov (2003), Malhotra et al. (2004) and Dinev and Hart (2004).

[13] That is, as already noted, it is possible that *ContrPref* is a poor proxy for *risk aversion*, not least because, as shown in Table 7 (see Appendix), it correlates too much to *perceived risk*.

we seek to gain at least some insight into the true relation between preference for control of personal information and privacy risk aversion. Taken at face value, the positive sign and lack of statistical significance of the coefficient of *Avail* (i.e., the dummy for the occurrence of a recent privacy breach) may suggest the absence of availability bias. This conclusion, however, might be premature as it can also be explained by a possible endogenity of this variable. It is, in fact, possible that individuals who are more willing to disclose personal information are more likely experience privacy breaches.[14] The positive and significant coefficient of *AmbAver* might also seem surprising. Taken at face value, this finding contrasts with the RPC model. This may be rationalized, however, by recognizing that, in our regression model, we face an unavoidable omitted variable problem. The RPC model posits a negative relation between willingness to disclose personal information and both *ambiguity* and *ambiguity aversion* but, as noted, our survey only measures attitudes and reported behaviour, rather than situation-specific circumstances. We therefore do not have, nor can have data on *ambiguity* but only on *ambiguity aversion*.[15] As already noted, this possible omitted variable problem is unavoidable, as we can only observe attitudes and their determinants, rather than reactions to specific circumstances or

[14] To control for this possibility, we would have to estimate a suitably identified system of simultaneous regressions, but such system would be highly unidentified unless data on actual information disclosure and privacy breach occurrences (as opposed to intentions to disclose information and reported occurrence of privacy breaches) were available.

[15] As it is typically the case in omitted variable problems, estimates of the coefficient of the included variable, i.e. *ambiguity aversion*, are biased and inconsistent if the omitted variable, i.e. the ambiguity of specific online environments, is correlated (due to sampling bias or for some underlying influence) with the included variable, i.e. *ambiguity aversion*. If the coefficient of both the included and the omitted variable were negative, as predicted by the RPC model, the correlation between the two variables would have to be negative to explain the observed positive coefficient of the included variable, i.e. of ambiguity aversion. It is plausible that the more ambiguity-averse individuals might deem the typical online interaction less ambiguous, possibly because of a tendency to avoid ambiguous situations in the first place.

environments. Finally, the fact that *Willingness* is negatively related to *ImpTrust* suggests that the greater the importance our subjects place on trust, the less inclined they are to disclose personal information when interacting online. This implies that our typical subject considers online environments relatively untrustworthy.

5.2.2 Model for risk-handling behavior

Regarding the model for *RiskHand*, the final specification includes all variables except *Avail*, i.e. the proxy for the availability of a recent negative experience, *Age* and *Work_comp*. All other variables enter the regression with an estimated sign that is consistent our RPC model, under the assumption that risk handling behaviour is costly. In particular, consistent with (H5) and (H6.b), our results suggest that the intensity of risk handling behaviour increases with the perceived benefit and perceived risk (*PerBen* and *PerRisk*) of online interaction, e.g. risk handling behaviour is especially beneficial when both the expected benefit and the risk of interacting is high. Therefore only a suitable combination of such circumstances warrants undertaking the cost. A subject's risk handling behaviour decreases with propensity to trust (*PropTru*) and ambiguity aversion (*AmbAver*). Also, as implied by the marginally negative coefficient of *Gender*, men are inclined to undertake somewhat less intense risk handling behaviour than women. These results are consistent not only with H5 and H6, in common to both the PC and the RPC models, but also with H7 and H8, which are not consistent with typical formulations of the PC model but are consistent with our augmented RPC version.

In the privacy calculus model, expected utility is a negative function of risk and a positive function of the expected benefit. Also, risk handling behaviour is, in one way or another, costly. Hence, as per our set of hypotheses, we would expect more intense

risk handling behaviour by subjects who, at one time, perceived the greatest risk and the greatest potential benefit from interactions in online environments (whereas, in the presence of high perceived risk but low expected benefit disengagement may be the rational choice). The fact that the declared intensity of the risk handling behaviour increases both with the perceived benefit and perceived risk is, therefore, in line with the privacy calculus model, both in the traditional formulation and in our revised one, and highlights the role played, in the decision of how to interact online, by the rational assessment of risks and benefits.

A somewhat similar line of reasoning applies to the interpretation of the coefficients of propensity to trust (*PropTru*) and importance placed on trust (*ImpTru*). Propensity to trust leads users to perceive a privacy threat as less likely whereas a greater importance placed on trust leads them to deem it more likely because, as inferred from the analysis of the estimated regression model for *Willlingness*, our typical user considers online environments relatively untrustworthy. Therefore, in agreement with the RPC model, expected utility of risk handling behaviour would be higher for a user with lower propensity to trust and who placed greater importance on trust. Such a user would be more inclined to undertake the costs required to deploy the risk handling behaviour. Similarly, for users with greatest preference for control, the expected utility of risk handling behaviour is also greatest, thus explaining the positive coefficient of *ContrPref*.

The negative coefficient of *AmbAver* is also consistent with our RPC model, in that the assumed reaction of individuals to ambiguity is simply withdrawal. That is, whereas a certain amount of risk handling behaviour is the optimal choice in the presence of privacy risk in that it improves the risk-reward profile of the decision to interact, the

optimal choice in the presence of ambiguity perception and of aversion to it (both indistinguishably captured by *AmbAver*) is not to undertake risk handling behaviour but to disengage altogether. It is therefore consistent with our ambiguity-augmented RPC model that subjects who are more averse to ambiguity undertake less, not more, risk handling behaviour. These results, therefore, extend Drennan et al.'s (2006) findings by suggesting that the opportunity to deploy privacy risk handling behaviour does not lead to increased online disclosure of personal information *in ambiguous scenarios*. Finally, the intensity of risk handling behaviour appears to be related to measures of limits to rationality, in that declared risk handling behaviour intensity is greater for users with greater education and familiarity with ICTs (as proxied for by *Home_comp* and *Comp_ind*).

Table 2 GLM Regressions
(Dependent variable: *Willingness*)

PerBen	*PerRis*	*PropTru*	*ImpTru*	*ContrPref*	*AmbAver*	*Avail*	*Age*	*Gender*	*Education*	*Home_comp*	*Work_comp*	*Comp_ind*	R^2
						PC model							
0.22	-0.36	-0.02	-0.55	-0.00									0.15
0.02	0.09	0.08	(0.21)	0.04									
(0.000)	(0.000)	(0.751)	(0.008)	(0.946)									
0.22	-0.24	-0.01	-0.45	0.02			-0.70	-0.01					0.27
0.03	0.08	0.06	0.20	0.07			0.08	0.10					
(0.000)	(0.002)	(0.887)	(0.019)	(0.783)			(0.000)	(0.913)					
						RPC model							
0.23	-0.25	-0.03	-0.41	0.02	0.02	0.00	-0.63	0.06	-0.25	1.97	0.67	-0.12	0.28
0.00	0.00	0.62	0.05	0.76	0.45	0.93	0.00	0.38	0.22	0.00	0.08	0.68	
(0.000)	(0.000)	(0.618)	(0.046)	(0.757)	(0.450)	(0.931)	(0.000)	(0.375)	(0.224)	(0.000)	(0.076)	(0.679)	

Notes. This table reports the estimates of unrestricted and restricted regressions of the dependent variable *willingness* against the regressors listed in the top row. The unrestricted regression includes all such variables. The restricted regressions include only a subset of such variables (or, equivalently, the coefficients of some of the regressors of the unrestricted model are set to zero). In the Table, the cells corresponding to the excluded regressors are left blank. The estimation method is GLM with clustered GLS standard errors. For all included regressors, we report the coefficient estimates followed by the associated standard errors and *p*-values (in brackets).

Table 3 GLM Regressions
(Dependent variable: *RiskHand*)

PerBen	*PerRis*	*PropTru*	*ImpTru*	*ContrPref*	*AmbAver*	*Avail*	*Age*	*Gender*	*Education*	*Home_comp*	*Work_comp*	*Comp_ind*	R^2
							PC Model						
0.04	0.09	-0.10	0.32	0.05									0.07
0.01	0.04	0.02	0.13	0.03									
(0.000)	(0.010)	(0.000)	(0.014)	(0.07)									
0.04	0.07	-0.10	0.31	0.06			0.08	-0.20					0.09
0.01	0.03	0.02	0.11	0.03			0.05	0.04					
(0.000)	(0.044)	(0.000)	(0.003)	(0.052)			(0.010)	(0.000)					
							RPC Model						
0.03	0.05	-0.09	0.18	0.06	-0.03	0.00	0.06	-0.08	0.14	1.66	-1.21	0.61	0.16
0.11	0.11	0.00	0.02	0.00	0.05	0.91	0.41	0.12	0.01	0.01	0.12	0.00	
(0.113)	(0.107)	(0.000)	(0.020)	(0.003)	(0.053)	(0.911)	(0.411)	(0.115)	(0.005)	(0.005)	(0.122)	(0.000)	

Notes. This table reports the estimates of unrestricted and restricted regressions of the dependent variable *RiskHand* against the regressors listed in the top row. The unrestricted regression includes all such variables. The restricted regressions include only a subset of such variables (or, equivalently, the coefficients of some of the regressors of the unrestricted model are set to zero). In the Table, the cells corresponding to the excluded regressors are left blank. The estimation method is GLM with clustered GLS standard errors. For all included regressors, we report the coefficient estimates followed by the associated standard errors and *p*-values (in brackets).

5.3 The 20 Semi-structured Interviews

Out of the survey participants, a total of 20 individuals agreed to participate in the semi-structured interviews, equally split across genders. The interviews were conducted two months after the questionnaire was completed. They were primarily carried out to better capture constructs that were weakly measured by the questionnaire, with special emphasis on those pertaining to the following subset of hypotheses:

Willingness to disclose personal information is:

- positively influenced by perceived control and trust in the counterparty/online situation (as negative antecedents of perceived risk), for a given level of risk aversion, and vice versa (H2.(a)).
- negatively influenced by positive antecedents to perceived ambiguity, such as the individual's age (H3.(a)).

Risk-handling behaviour is:

- negatively impacted by negative antecedents of perceived risk, such as perceived control and trust, for given propensity to trust in online situations (H6.(a)).
- negatively impacted by perceived ambiguity and possible positive antecedents thereof, such as age (H7.(a)).

Another key purpose of the interviews was to help ascertain whether ambiguity and ambiguity aversion are negatively correlated, so as to clarify whether the surprisingly positive (and significant) sign of the ambiguity aversion coefficient in the regression model for willingness to disclose personal information can be explained as a

consequence of the (un-modelled) omission of ambiguity from amongst the regressors.

5.3.1 The Demographics of the Respondents

Out of the 20 focus group participants, there were two respondents between 18-24 years and four individuals over 55 years, which left fourteen individuals within the age group of 25-54 years. Sheehan's (2002) four-part typology for the classification of individuals according to their privacy tendencies was used to group the respondents, i.e. the privacy unconcerned, the circumspect, the wary, and the privacy alarmed. The respondents were categorised according to their responses to questions that were taken from previous research (Sheehan, 2002). All four categories were present among the 20 respondents. Figure 3 shows the breakdown of the number of respondents according to this classification. In figure 4, we see that the circumspect Internet users reportedly experienced the most privacy breaches followed by the wary Internet users. Interestingly, the alarmed Internet users experienced no previous informational privacy breaches.

Figure 3 Respondents according to Sheehan's (2002) privacy classification

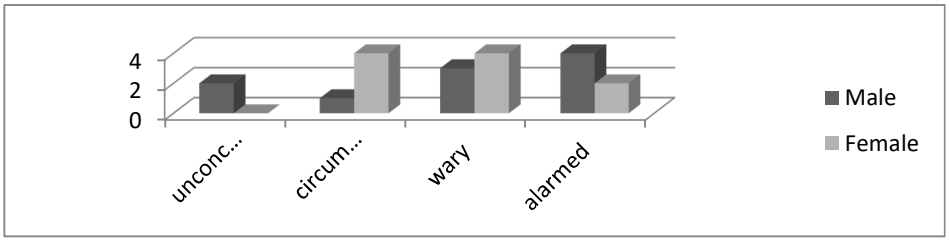


Figure 4 Respondents who have experienced a privacy breach in the past

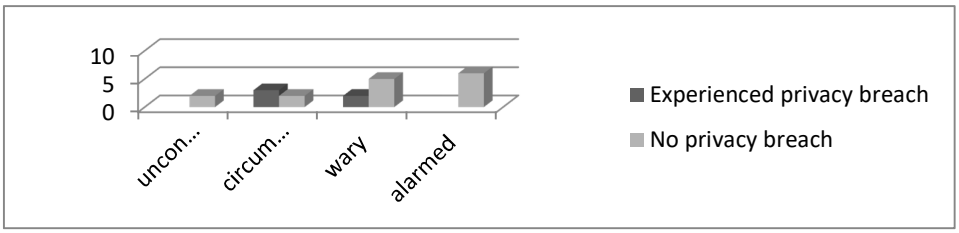
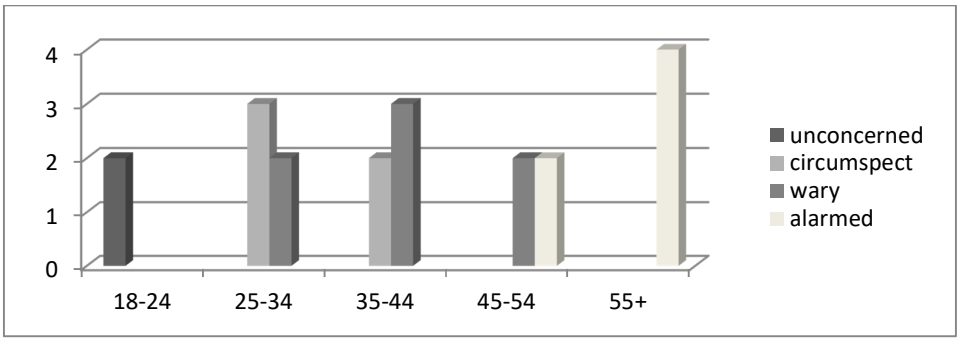


Figure 5 shows the breakdown in ages among the respondents. It is interesting to note that, as age increases, so too does privacy risk perception, as captured by the classification.

Figure 5 A breakdown of respondents according to age and privacy risk perception



5.3.2 Findings from the Interviews

As noted, one key purpose of the interviews was to help ascertain whether ambiguity and ambiguity aversion are negatively correlated. The interview findings support this conclusion, through the relation of both constructs with risk taking and risk handling behaviour, in that those who have the greatest aversion for ambiguity (i.e., the subjects

who were classified as concerned and alarmed) also reported experiencing privacy breaches less frequently (Figure 5), because of a lower propensity to take risk or, at least, a greater propensity to handle it carefully. That is, it appears that ambiguity and ambiguity aversion are indeed negatively correlated in that individuals who are averse to ambiguity systematically avoid ambiguous situations, ending up perceiving the online context in which they interact as less ambiguous. That is, in the structural model for willingness to disclose personal information, the omitted variable ambiguity is endogenous and negatively influenced by an included variable, ambiguity aversion. This is important as it permits us to conclude that the positive sign of the estimated coefficient of ambiguity aversion in the regression model for willingness to disclose personal information does not represent evidence against the RPC model but is due instead to inconsistency of the coefficient estimate due to an (unavoidably) omitted variable negatively correlated with ambiguity aversion.

According to eleven out of the twenty interviewees, risk handling behaviour is reportedly only carried out on websites that are (up to that point) not trusted and, as a result, are seen to pose a potential risk if they require the submission of personal information. These eleven interviewees stated that, if they trust a site, there is minimal or no need to carry out risk handling behaviour. The risk handling behaviour is conducted to eliminate or reduce perceived risk of an (as of yet) untrusted site to an acceptable level so that disclosure can take place. Overall, these findings can be interpreted as indicating that, once a website is deemed trustworthy, individuals are willing to disclose personal information, essentially regardless of available risk handling behaviour options, consistent with H6.(a).

All respondents admitted to refraining from submitting personal information in the presence of ambiguity, consistent with H3.(a). In fact, one 55+ "alarmed" male admitted to doing the following in the presence of ambiguity:

> *"I have even driven 7 hours round trip to check out a potential supplier before I decided to deal with them online. I needed to check out their premises and check them out, you know…what they are like as people, before I felt confident to deal with them virtually"*

All "alarmed" internet users, all in the 35+ age brackets, said that they place little or no emphasis on trust and indeed undertake minimal risk handling behaviour, rather preferring to abstain from submitting personal information online completely whenever possible, consistent with both H3.(a) and H6.(a). This finding also reflects the findings from the online questionnaire that the greater the importance placed on trust by respondents the more risk handling behaviour they undertake, i.e. the younger internet users place more emphasis on trust in online contexts and therefore engage more in risk-handling behaviour, consistent with H6.(b). From the interviews, none of these "alarmed" Internet users were under the age of 35, supporting H3.(a) and H3.(b) that age has a negative impact on users' willingness to disclose personal information in perceived ambiguous online situations, and suggesting that this relation is mediated by the importance placed on trust, consistent with H2.(b).

Age has a positive impact on both perceived ambiguity and ambiguity aversion, supporting the conjecture we put forth in formulating H3.(a) and (b) and H7.(a) and (b). In particular, there was a distinct difference in the perception of ambiguity between the different age groups, with older respondents appearing more prone to perceive ambiguity in a given situation, and ambiguity aversion was strongest among

the older age groups for both willingness to disclose personal information and their risk handling behaviour intensity.

Repeatedly, the importance an individual places on trust has a positive impact on the intensity of the individual's risk handling behaviour. That is, when facing a not yet trusted online counterparty, an individual who deems trust to be of a high importance tends to undertake risk handling behaviour, to see if trust can be built, rather than disengage (suggesting that trust and risk handling behaviour are complements rather than substitutes). To the extent that the importance placed on trust is a valid proxy for risk aversion, this is consistent with H6.(b).

Risk handling behaviour takes place when individuals believe the risks of the online situation are quantifiable and can be reduced by such behaviour. That is, consistent with H7.(a) and H7.(b), risk handling behaviour does not take place in the presence of ambiguity (in such case individuals perceive the privacy risks to be unquantifiable and prefer to refrain from disclosing personal information online). If the benefit from online interaction is high enough, some alarmed individuals defer to a trusted third party to carry out the interaction, i.e. a computer expert or, as one "alarmed" lady put it,

> *"My son knows all about computers so I let him take care of the things I would be too scared to do. I know we have to book our flights online so he always does that for me as he knows how to do it safely"*

On a related note, the interviews confirmed that individuals' level of education and their familiarity with ICTs has a positive impact on their propensity to engage in privacy risk handling behaviour. This is broadly in line with the RPC model in that

education and familiarity with ICTs reduce limits to rationality and therefore perceived ambiguity (H7.(c) and H8 respectively).

Evidence of cognitive biases was found directly in the responses of nine respondents. In fact these respondents unequivocally indicated their reliance on heuristics when making decisions concerning their informational privacy. Table 4 gives a breakdown of respondents' biases found from discussions with them:

Table 4 Breakdown of heuristic biases among respondents

***Respondent's* classification**	*unconcerned*	*circumspect*	*Wary*	*Alarmed*
Biases				
Anchoring and adjustment	1	1		
Representativeness bias		2	3	
Availability bias		1		1

Notes: Anchoring and adjustment refers to evidence that respondents based their decisions on first impressions of a website or the initial look and feel of the site. Representativeness and availability bias refer to the tendency for the respondents to make decisions based on what they hear from the media and how recently they have heard it.

Overall, our findings support that, consistent with the RPC model, individuals do not undertake risk handling behaviour 1) when their trust propensity is high and 2) in ambiguous circumstances. This indicates that individuals do not see the need for risk handling behaviour when they either do not perceive risk is sufficiently high to warrant such behaviour (high trust propensity) or conversely they perceive so much risk that risk handling behaviour is deemed pointless (the risks are so high that they are perceived as unmanageable and the situation is, as a consequence, perceived as essentially ambiguous).

6. Conclusions and Final Remarks

In this paper, we extend the privacy calculus model by explicitly allowing for behavioural biases and aversion to ambiguity, drawing on the literature on limits to

rationality and on insights for behavioural economics. Based on a survey of Irish IS users and of twenty semi-structured interviews carried out two months after the online questionnaire, we find support for the implications of the model, especially when contrasted with the implications of more traditional and restricted versions that do not take limits to rationality and ambiguity aversion into account.

An important finding from both the questionnaire and the interviews is that, in the face of ambiguity, both the willingness to disclose personal information and the propensity to engage in privacy risk handling behaviour decrease. This indicates that privacy risk handling behaviour takes place only in the presence of uncertainty of the "quantifiable" sort, i.e. risk, in an effort to reduce that risk to an acceptable level. In the presence of ambiguity or "unquantifiable" risk, risk handling behaviour is seen as pointless.

The intellectual underpinning of the PC model is the conceptualization of privacy as a condition with a relative rather than an absolute value. It can be argued, however, that the model can be viewed, in a sense, as encompassing both views. From this point of view, an individual who views privacy as a condition carrying an absolute (rather than a relative) value could be characterized as exhibiting an infinite privacy risk aversion or, equivalently, as perceiving an infinite amount of privacy risk. The implication of this characterization is that such an individual would never willingly put privacy at risk, exactly what we would expect from an individual who deemed privacy an absolute. This interpretation of the implications of viewing privacy as an absolute is however problematic. For example, it might be argued that there are always situations in which even the most privacy loving individual would sacrifice his or her privacy, e.g. if the choice were between the latter and, say, the well-being of a close relative. In the

context of the RPC model, a more nuanced approach to the characterization of an individual who deems privacy to be an absolute might therefore envisage that privacy is not the only condition to which the individual associated an infinite amount of risk and/or benefit. While fascinating, however, we leave a further exploration of the implications of viewing privacy as an absolute to future research.

Bibliography

Acquisti, A., 2009. Nudging privacy: The behavioral economics of personal information. *IEEE Security and Privacy,* 7(6), pp. 82-85.

Acquisti, A. & Grossklags, J., 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy,* Volume 1, pp. 26-33.

Acquisti, A. & Grossklags, J., 2008. What Can Behavioral Economics Teach Us About Privacy?. In: *Digital Privacy: Theory, Technologies, and Practices.* Boca Raton, Florida: Auerbach Publications.

Anand, P., 2002. *Foundations of Rational Choice Under Risk*. third ed. Oxford, UK: Oxford University Press.

Arona, R., Sundararajanb, A. & Viswanathan, S., 2006. Intelligent agents in electronic markets for information goods: customization, preference revelation and pricing. *Decision Support Systems,* 41(4), p. 764–786.

Chellappa, R. K. & Shivendu, S., 2007. An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization. *Journal of Management Information Systems,* 24(3), pp. 193--226.

Chellappa, R. K. & Shivendu, S., 2010. Mechanism Design for "Free" but "No Free Disposal" Services: The Economics of Personalization Under Privacy Concerns. *Management Science,* 56(10), p. 1766–1780.

Chellappa, R. K. & Sin, R. G., 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management,* 6(2), pp. 181-202.

Cohen, J. E., 2001. Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. *Georgetown Law Journal,* Volume 89.

Davis, M., 2010. *Towards a Political Economy of the Internet*. [Online]
Available at: http://vimeo.com/channels/129520
[Accessed 6 May 2011].

Dineva, T. & Hart, P., 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology,* November , Volume 23(Issue 6), pp. pages 413 - 422.

Dinev, T. et al., 2006. Privacy Calculus Model in E-Commerce: A Study of Italy and the United States. *European Journal of Information Systems,* 15(4), pp. 389-402.

Drennan, J., Mort, G. S. & Previte, J., 2006. Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users. *Journal of Organisational and End User Computing,* 18(1), pp. 1-22.

Erbas, N. & Mirakhor, A., 2007. The Equity Premium Puzzle, Anbiguity Aversion, and Institutional Quality. *IMF Working Paper: work in progress, Washington DC: International Monetary Fund.*

Federal Trade Commission, 2010. *Protecting Consumer Privay in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.* [Online]
Available at: http://ftc.gov/os/2010/12/101201privacyreport.pdf
[Accessed 13 May 2011].

Forrester Research, 2010. *North American Technographics® Benchmark Survey, Q2 2010 (US, Canada).* [Online]
Available at:
http://www.forrester.com/North+American+Technographics+Benchmark+Survey+Q2+2010+US+Canada/-/E-SUS787
[Accessed 14 April 2012].

Gigerenzer, G. & Selten, R. eds., 2002. *Bounded Rationality: The Adaptive Toolbox*. London, England: The MIT Press.

Hann, I. H., Hui, K. L. & Lee, S. Y. T., 2008. Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems,* 24(2), pp. 13-42.

Hann, I.-H., Hui, K.-L., Lee, T. S. & Png, I., 2008. Consumer Privacy and Marketing Avoidance: A Static Model. *Management Science,* 54(6), pp. 1094 - 1103.

Hui, K. L., Teo, H. H. & Lee, S. Y., 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly,* Volume 31, pp. 19-33.

Johnston, C., 2012. *Google paying users to track 100% of their Web usage via little black box*. [Online]
Available at: http://arstechnica.com/gadgets/2012/02/google-paying-users-to-track-100-of-their-web-usage-via-little-black-box/
[Accessed 1 May 2012].

Kahneman, D. & Tversky, A., 1972. Subjective probability: A judgment of representativeness. *Cognitive Psychology,* Volume 3, pp. 430-454.

Kahneman, D. & Tversky, A., 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica,* Volume 48, pp. 263-291.

Knight, F. H., 1921. *Risk, Uncertainty, and Profit*. Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Company.

Lessig, L., 2000. Code is Law: On Liberty in Cyberspace. *Harvard Magazine,* pp. Available at: http://harvardmagazine.com/2000/01/code-is-law-html.

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), pp. 336-355.

Muth, J. F., 1961. Rational Expectations and the Theory of Price Movements. *Econometrica,* 29(3), pp. 315-335.

Peter, J. P. & Tarpey, L. Z. S., 1975. A Comparative Analysis of Three Consumer Decision Strategies. *Journal of Consumer Research,* Volume 2, pp. 29-37.

Posner, R. A., 1978. An Economic Theory of Privacy. *AEI Journal on Government and Society,* May/June.pp. 19-26.

Shefrin, H., 2002. *Beyond Greed and Fear*. New York: Oxford University Press.

Simon, H., 1957. A Behavioral Model of Rational Choice. In: *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*. New York: Wiley.

Smith, H. J., Dinev, T. & Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly,* 35(4), pp. 989-1015.

Stone, E. F. & Stone, D. L., 1990. Privacy in organizations: Theoretical issues, research findings and protection strategies. In: *Research in personnel and human resource management*. Greenwich, CT: JAI Press, pp. pages 349-411.

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), pp. 254-268.

von Neumann, J. & Morgenstern, O., 1947. *Theory of Games and Economic Behavior*. 2nd ed. Princeton, NJ: Princeton University Press.

Westin, A., 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues,* Vol 59((2)), pp. pp. 431-453.

Wilson, D. W. & Valacich, J. S., 2012. *Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus*. Orlando 2012, s.n.

Xu, H., Teo, H. H. & Tan, B. C. Y., 2010. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems ,* 26(3), pp. 137-176.

Xu, H., Teo, H. H., Tan, B. C. Y. & Agarwal, R., 2009. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems,* 26(3), pp. 135-173.

Appendix: The Questionnaire (Mapping between Survey Questions and Constructs)

The majority of questions in the questionnaire were drawn from existing instruments cited within the literature, but modified to reflect the needs of this research. Given the difficulty of forming a sample representing the 'true' population, or even of defining ex-ante an appropriate sampling scheme, we also asked the respondents to provide information on variables that may be correlated with un-modelled socio-demographic influences on attitudes to privacy. These variables were to be used as control variables in the empirical testing of the privacy calculus model.

The set of questions in the online questionnaire is summarized in Table 6 (which continues over a number of pages). From the questionnaire, we sought to sample proxy measures for nine constructs, i.e. (1) willingness to disclose personal information (*Willingness*), (2) perceived benefit from doing so (*PerBen*), (3) perceived risk (*PerRis*) in doing so, (4) propensity to trust (*PropTru*), (5) importance placed on trust (*ImpTru*), (6) control preferences of subjects (*ContPref*), (7) ambiguity aversion (*AmbAver*), (8) availability bias (*Avail*) and (9) extent of (or propensity to engage in) risk handling behaviour (*RiskHand*). The questions on constructs (1) to (8) are based on the questions drawn from the literature and adapted as explained in a separate Appendix, available from the authors upon request, whereas the questions on construct (9) are, to our knowledge, novel.

We employed different scale endpoints and formats for the criterion (*Willingness* and *RiskHand*) and predictor (all other variables) measures in order to reduce method biases caused by commonalities in scale endpoints and anchor effects. Additionally, to make common method bias less likely, we varied the order of questions relating to different scales and constructs, to reduce the likelihood of the respondents combining related items to produce a biased pattern in their responses (Murray, Kotabe, & Zhou, 2005). On a related note, we used different response anchors across measured constructs and manipulated the order of questionnaire items in such a way that common method variance across dependent, independent and control variables became less likely.

We use the survey results to generate variables representing instruments for each one of the nine constructs. The construction of the key variables is summarized in the last column of Table 5. Table 6 reports summary statistics for many of these variables and Table 7 reports pairwise sample correlations between them. As can be seen from Table 7, Panel A, willingness to disclose appears to be highly positively correlated with perceived benefit and negatively correlated with perceived risk. Age, education and the availability bias proxy, which is the dummy variable indicating whether the participant has experienced a privacy breach in the last six months, are also all negatively correlated with willingness to disclose personal information. From Panel B of the same Table, which reports robust (conservative) Bonferroni-adjusted *p*-values of the test that the pairwise correlation is equal to zero, we see that willingness to disclose personal information is significantly correlated to perceived risk, perceived benefit, age and education. Notably, the risk handling behaviour instrument appears to be correlated to a significant extent to all variables, as shown in Panel A of Table 7. As suggested by the more conservative Bonferroni p-values reported in Panel B of this

Table, however, the most significant association appears to be with the instruments for working on a computer at work and working in the computer industry. There are a number of significant correlations between various other variables suggesting that disentangling causality relations from mere correlations and (direct or indirect) reverse causality might be especially challenging. The instrument for ambiguity aversion (*AmbAver*) is highly positively correlated with age. The perceived risk instrument (*PerRis*) is negatively correlated with the instrument for propensity to trust (*PropTru*), suggesting that the two instruments might be measuring, at least to some extent, the same construct. We shall seek to overcome this problem in the specification of the multiple regression model. It is hoped that, by simultaneously controlling for different, albeit imperfectly measured effects, their statistical identification will be possible.

Table 5 Questionnaire Constructs and Associated Proxy Variable

Questions Included in the Questionnaire for Each Construct and Associated Proxy Variable

	Construct	*Associated Questions*	*Associated Proxy Variable*	*Proxy Variable Definition*
1	**Willingness to disclose personal information**	(a) I submit my personal information online in exchange for taking part in social networking; (b) I submit my personal information online in exchange for taking part in discussion forums; (c) I submit my personal information online in exchange for being in with a chance to win something; (d) I submit my personal information online in exchange for carrying out official activities such as online voting	$Willingness_i$	$Willingness_i$ = (a) + (b) + (c) + (d)
2	**Informational control preference (proxy for risk aversion)**	(a) To me online privacy is being able to control how my personal information is used; (b) To me online privacy is being able to feel confident that my personal information is safeguarded against inappropriate sale or loss; (c) My online privacy is threatened if I don't feel fully in control of the situation; (d) When disclosing personal information online it is more important to be in control of how it is collected, used and shared than to trust the online third party to whom it is being submitted	$ContrPref_i$	$ContrPref_i$ = (a) + (b) + (c) + (d)
3	**Ambiguity Aversion**	When I am asked to supply personal information in order to obtain a service that I need on a website and I feel that information is unnecessary, the website should: (a) Make the submission of that private information "optional"; (b) Explain clearly why I need to submit the personal information in return for the service I am seeking; (c) Have a clear statement that is readily accessible on the site of how a user's personal information will be used; (d) Provide a means of contacting the company to express your view or make a complaint	$AmbAver_i$	$AmbAver_i$ = (a) + (b) + (c) + (d)
4	**Perceived risk**	When submitting personal information online (a) There is risk involved; (b) There is potential for loss; (c) Many unexpected problems can arise	$PerRis_i$	$PerRis_i$ = (a) + (b)

5	**Perceived benefit**	(a) When submitting personal information online, the benefits outweigh the risks (b) I submit my personal information online in exchange for the convenience of being able to bank online; (c) I submit my personal information online in exchange for the convenience of being able to shop online; (d) I submit my personal information online in exchange for paying bills; (e) When submitting personal information online, there is potential for gain	$PerBen_i$	$PerBen_i$ = (a) + (b) + (c) + (d) + (e)
6	**Propensity to trust**	(a) In general, my perception of online companies is that they are mindful of my best interests when handling my personal information; (b) In general my perception of online companies is that they are truthful about their use of my personal information; (c) In general my perception of online companies is that they are motivated by their best interests, rather than mine, when handling my personal information; (d) In general my perception of online companies is that they are secretly collecting, using and selling personal information for their own competitive advantage; (e) When disclosing personal information online it is more important to trust the online third party to whom it is being submitted because it is important to be fully in control of how it is collected, used and shared	$PropTru_i$	$PropTru_i$ = (a) + (b) + (c) - (d)
7	**Importance placed on trust**	(a) In general, my perception of online companies is that they are mindful of my best interests when handling my personal information; (b) In general my perception of online companies is that they are truthful about their use of my personal information; (c) In general my perception of online companies is that they are motivated by their best interests, rather than mine, when handling my personal information; (d) In general my perception of online companies is that they are secretly collecting using and selling personal information for their own competitive advantage; (e) When disclosing personal information online it is more important to trust the online third party to whom it is being submitted because it is important to be fully in control of how it is collected, used and shared	$ImpTru_i$	$ImpTru_i$ = (e)
8	**Potential for availability bias**	How often in the past 6 months have you experienced a potential threat to your online privacy?	$Avail_i$	$Avail_i$ = (a)
9	**Risk handling behaviour**	In general, what measures do you take to safeguard your personal information from online privacy threats (all 0/1 binary scores):	$RiskHand_i$	$RiskHand_i$ = - (a) + (b) + (c) + (d) + (e) + (f) + (g)

		(a) I take no measure; (b) I contacted the offending third party; (c) I submit inaccurate or incomplete information; (d) I conduct extensive searches to find the most reliable sources with whom to interact; (e) I buy online only from well-known and trusted brands; (f) I check the privacy statements/policies of websites before submitting an personal information; (g) I check for privacy seals and security settings of websites; (h) I only interact with websites that I trust; (i) I use word of mouth to find reliable websites with whom to interact		
10	**Age**	How old are you?	Age_i	Integer numeric value of answer
11	**Sex**	Are you male/female?	$Gender_i$	1 for male and 0 for females
12	**Education level**	What was the last year in school/college that you completed? (a) Junior/Inter Certificate; (b) Leaving Certificate (or equivalent); (c) Some college (1-3 years); (d) College graduate (degree level); (e) Postgraduate (degree +); (f) Prefer not to answer	Education	Integer numeric value of answer
13	**Home computer**	Do you have a computer at home?	Home_comp	1 for yes and 0 for no
14	**Work computer**	Does your work involve spending time on a computer?	Work_comp	1 for yes and 0 for no
15	**Employed in the computer industry**	Do you work in the computer industry?	Comp_Indust	1 for yes and 0 for no

Table 6
Summary Statistics

Variable	Obs	Mean	Std.Dev.	Min	Max
Willingness	372	3.67	2.35	0	12
RiskHand	419	3.56	1.34	0	7
ContrPref	383	10.21	2.32	0	12
AmbAver	419	18.88	2.99	10	25
PerRis	411	6.59	1.19	2	8
PerBen	371	12.72	3.56	0	20
PropTru	419	-0.33	2.00	-9	5
ImpTru	376	1.53	0.50	1	2
Avail	419	3.10	2.16	0	6
Age	371	3.39	1.16	1	6
Education	367	5.13	1.01	2	6
Home_comp	370	0.99	0.10	0	1
Work_comp	373	0.99	0.12	0	1
Comp_ind	370	0.24	0.42	0	1

Notes. This table reports summary statistics, i.e. number of available observations, sample mean and sample standard deviation, minimum and maximum, for the constructed instruments and for the demographic variables.

Table 7 Correlation Matrix

Panel A

	Willingness	RiskHand	ContrPref	AmbAver	PerRis	PerBen	PropTru	ImpTru	Avail	Age	Gender	Education	Home_comp	Work_comp	Comp_ind
Willingness	100.00														
RiskHand	-7.44	100.00													
ContrPref	-1.72	**13.81	100.00												
AmbAver	-3.37	**-12.99	**16.11	100.00											
PerRis	**-19.93	**11.38	**15.33	**10.64	100.00										
PerBen	**31.73	**10.97	-2.28	2.36	-7.83	100.00									
PropTru	7.65	**-10.28	*-9.26	**12.72	**-17.93	**13.39	100.00								
ImpTru	-6.70	**11.15	-6.51	-1.23	2.90	**16.01	**11.09	100.00							
Avail	*-9.77	**10.36	5.46	**-22.02	**14.54	**-13.32	**-11.42	-2.31	100.00						
Age	**-37.26	**12.74	7.38	**19.37	**18.89	-0.31	-3.96	4.61	*8.83	100.00					
Gender	5.07	*-8.65	0.06	**11.95	-7.70	6.47	*9.27	-0.40	-2.74	-5.95	100.00				
Education	**-27.75	**17.21	4.15	**16.34	**17.02	*10.12	**-11.03	7.46	5.50	**48.98	6.71	100.00			
Home_comp	6.55	**11.02	6.76	6.63	5.06	-0.85	3.24	0.66	-1.88	3.05	-3.74	7.23	100.00		
Work_comp	6.90	**-18.05	1.86	-1.63	-3.74	-3.78	**10.52	-7.82	3.67	2.07	-1.46	**-10.94	1.23	100.00	
Comp_ind	0.95	**22.47	2.27	0.30	5.33	**16.70	7.67	**17.26	-2.53	-2.08	**-22.10	0.92	-0.44	-6.43	100.00

Panel B

	Willingness	RiskHand	ContrPref	AmbAver	PerRis	PerBen	PropTru	ImpTru	Avail	Age	Gender	Education	Home_comp	Work_comp	Comp_ind
Willingness															
RiskHand															
ContrPref															
AmbAver															
PerRis	0.027														
PerBen	0.000														
PropTru					0.055										
ImpTru															
Avail				0.002											
Age	0.000			0.024	0.035										
Gender															
Education	0.000									0.000					
Home_comp															
Work_comp		0.094													
Comp_ind		0.002									0.006				

Notes. Panel A of this table reports the matrix of percentage pairwise correlation coefficients, each estimated the largest available number of observations, for the variables indicated in the first row and column. One and two asterisks denote significance at the 10 and 5 percent significance level. Panel B reports robust (conservative) Bonferroni-adjusted *p*-values of the test that the pairwise correlation is equal to zero. To improve legibility, we report only *p*-values not exceeding 10 percent, i.e. only those that indicate rejection at least at the 10 percent level of the null hypothesis of zero correlation. All variables are denoted as in the text.