Online consumer privacy concern and willingness to provide personal data on the internet

Caroline Lancelot Miltgen

ONLINE CONSUMER PRIVACY CONCERN AND WILLINGNESS TO PROVIDE PERSONAL DATA ON THE INTERNET

CAROLINE LANCELOT MILTGEN
ASSISTANT PROFESSOR
UNIVERSITY OF ANGERS

Department of Law, Economics and Management
Groupe de Recherche Angevin en Economie et Management (GRANEM)
13, Allée François Mitterrand
BP 13633
49036 Angers Cedex 01
caroline.miltgen@univ-angers.fr

ABSTRACT

Our research examines the manner in which Web users choose between participation in the Internet economy and protection of their personal data. We study the influence of various contextual elements (e.g. the privacy policies posted on sites) and individual characteristics (e.g. privacy concern) on willingness to communicate personal data online. An experimental study carried out on a sample of French students provides the framework for testing a conceptual model. The impact of privacy concern on Web users' attitude is confirmed. Privacy policies and the amount of data requested are also shown to influence willingness to self-disclose. Finally, our findings establish that situational factors have a greater impact on the decision to provide personal data than personal convictions.

Key words: Privacy, personal data, the Internet, consumer behavior, self-disclosure

International Journal of Networking and Virtual Organisations (IJNVO)

Volume 6 - Issue 6 – 2009
p 574 – 603

Special Issue on Privacy in a Virtual Environment: Theory and Practice
Guest Editor: Dr. Regina Connolly

DOI: 10.1504/IJNVO.2009.027790

Direct link to the article:
http://www.inderscience.com/search/index.php?action=record&rec_id=27790&prevQuery=&ps=10&m=or

INTRODUCTION

A growing number of companies are attempting to collect individual-specific consumer data as part of their strategy to acquire and/or retain customer loyalty, the aim being to attract consumers with offers tailored to their individual tastes and needs. This practice has become increasingly wide-spread — particularly on the Internet (with its "clickable" data entry forms) — despite the Web's inherent tendency to exacerbate both risks of privacy invasion and consumers' fears of disclosing information, especially that of a sensitive nature. Beyond the strategic importance of collecting customer data, a twofold challenge has emerged: statutory (as pertains to the law) and, above all, ethical (as pertains to respecting individual privacy concerns). The literature, along with observation of real-life practices indeed shows that large numbers of consumers, wary of situations in which information is requested, refuse to disclose their personal data. This is often due to the impression that their privacy is being invaded, or because they fear the consequences of providing personal information; more specifically, consumers are afraid that the data they have voluntarily provided will be wrongfully used. Yet little is known for the moment about the way in which consumers actually perceive this type of data gathering and what then drives their decision to communicate personal data or not.

How consumers balance taking part in e-commerce and protecting their personal data is particularly unclear. The goal of our contribution is therefore to investigate the influence of different situational elements (e.g. consumer privacy policies displayed on sites) and of individual elements (e.g. the concern over protecting personal data) on Web users' attitudes when confronted with personal data gathering requests on the Internet.

After reviewing the literature on privacy concerns and willingness to disclose personal data on the Internet, we propose a conceptual model designed to measure the relative influence of individual and situational elements on consumers' willingness to provide information. We then outline the methodology and report the findings of our study, before going on to discuss the implications, limitations and further avenues of research stemming from our conclusions.

THE THEORETICAL UNDERPINNINGS OF OUR RESEARCH

Our research draws upon a number of concepts, presented hereafter: individual privacy concern, the perceived attributes of data gathering requests, and finally consumer attitude in reaction to disclosure of the data requested.

We also present the Theory of Reasoned Action (Fishbein and Ajzen 1975), the underlying theme to our thinking and to the elaboration of this study's conceptual model.

Privacy concern

The term *privacy* is commonly used to describe the combined needs for personal space and visual, physical or psychological separation, as well as control over one's personal property and data. Establishing a definition of this concept is nevertheless a tricky task, there being no general consensus on the subject. There are in fact a variety of conceptualizations, depending on which criteria — legal, social or political — are retained. When first described by Warren and Brandeis (1980), the construct of *privacy* was formulated as the right to be left alone. Several other definitions have since been put forward, fitting into three categories based on the aspect emphasized, whether physical (the right to retract), information-based (control over personal information) or relationship-based (control over social interactions).

Numerous theorists confine privacy to information-based aspects, i.e. a person's ability to limit access to his/her personal data. The most prevalent definition of this principle is the one given by Westin (1967): "the claim for individuals […] to determine when, how and to what extent information about themselves is communicated to others." Seen from this perspective, individuals are thus protected when they are able to manage the impressions they create with the information they provide. This entails the selective disclosure of information and the ability to regulate the dissemination of this data (Jourard 1966).

It is mainly this information-based dimension that comes into play when companies collect information. Indeed, a conflict exists between consumers' right to control subsequent use of personal data provided and companies' right to use this information for commercial purposes. This is an important issue, involving one of the factors most likely to influence consumers' response when asked to disclose information: the level of concern over privacy (or rather, over protecting their personal data[1]).

Most research indeed confirms the impact of privacy concerns[2] on consumers. Culnan and Armstrong (1999) demonstrate that concerned individuals are much more reluctant to provide personal data, findings confirmed by Farag and Krishnan (2003). In a similar manner, Phelps, Nowak and Ferrell's findings (2000) show a strong link between consumers' level of concern and beliefs about business practices on the one hand, and subsequent consumer behaviors on the other hand. Indeed, concerned individuals are more likely to disapprove of a company retaining information about them, and will more frequently request that their names be

[1] Defined as the level of concern individuals may feel when their privacy is invaded by companies requesting and/or making use of their personal data.

[2] In the text we use the acronym *PC* on occasion to designate the concept of privacy concern

removed from company files. Recent studies, however, emphasize the fact that some individuals, when online, put aside these concerns and tend to disclose information — even if the questions asked are of a personal nature, and even when there is no objective reason to do so. Other work indicates that consumers are becoming increasingly confident that their privacy will be respected on the Internet. Moreover, in spite of the concerns voiced by consumers, it is a documented fact that only 6 % of Web users surveyed felt that their privacy had actually been invaded (FTC 1998). What is more, a large number of individuals have come to realize the necessity of giving up a small portion of their privacy if they wish to engage in e-commerce (Gandy 1993). Because of the ease and value for money that they offer, online transactions indeed seem well on the way — in some cases at least — to overcoming Web users' privacy concerns. It therefore seems that consumers, despite the security risks and erosion of data protection, may act in a manner that belies predictions based on their level of concern over privacy.

Evaluation of Data Gathering Requests and the Response Process

Smith (1995) provides a partial explanation for this phenomenon when reporting that individuals are likely to adjust their level of concern to specific situations. For Dommeyer and Gross (2003), only a few consumers consider any and all information requests to be an encroachment on their privacy and most of them are willing to provide a certain amount of data under some circumstances. Hence, if consumers sometimes provide more data than their general level of concern would lead one to expect, it is because the behaviors they adopt are also (and perhaps mostly) dependent on the actual situation, e.g. the type of information requested; the terms under which the data is acquired; the safeguards for confidentiality; the benefits obtained in exchange — in other words, a set of factors which will only have an impact in a real-life situation and which depend on how they are actually perceived.

The model proposed by Olson and Dover (1978) establishes a link between exposure to a stimulus (in our case, a data request — here, the data entry form to be completed) and the beliefs that individuals have formed about it. This model is similar to the one stemming from the Theory of Reasoned Action (TRA) developed by Fishbein and Ajzen (1975), used to study the behavioral determinants of conscious decision-making. Their theory seems particularly well–adapted to examining the factors influencing an individual's response to requests for personal data.

Using the TRA model as a basis, an individual's response process when confronted with data gathering requests can be divided into 4 phases. When the Web user is asked to provide personal information (by accessing the page containing the data-entry form to be completed), he/she will very likely evaluate the request (belief formation) using the attributes perceived in relation to the set of elements characterizing the situation. Once this evaluation is complete, the individual is then likely to develop an attitude (either favorable or unfavorable) about communicating this data that will determine his/her behavioral intention to respond (likelihood that he/she will provide the data). This will in turn determine his/her real behavior, should an actual request occur. The variable central to this process is therefore attitude, which we have defined in the usual manner as the reaction of an individual towards an object (here, communicating data) in a favorable-unfavorable or like-dislike continuum (Fishbein and Ajzen 1975). In our study, attitude constitutes the dependent variable of our model and we therefore focus on the first two phases of the response process. Firstly, the factors related to the stimulus — i.e. the data entry form to be completed — and the manner in which the data gathering request is made (situational factors) are likely to have an impact on the individual's perception of the data gathering request. This evaluation may then induce the individual to develop a more or less favorable attitude towards data disclosure. Moreover, this attitude will be even more favorable if the evaluation is positive.

This thus leads to identifying two routes likely to influence attitudes toward data disclosure: an "individual" route represented by the influence of individuals' privacy concerns and a "situational" route corresponding to the influence of situational elements. The question now naturally arises as to which of these routes the consumer will prefer. The fact that consumers — though in principle concerned about privacy and therefore reluctant to disclose personal information — increasingly agree to disclose information even when it is avoidable, demonstrates the importance of situation and the way in which it is perceived. The study we are undertaking will allow us to provide a preliminary answer to this question.

We will now address the conceptual framework of our research. We will begin with the hypothesis linked to the effect of situational elements (H1 and H2) before going on to discuss those relating to the impact of privacy concerns (H3). Among others, the theory on motivation and expected outcomes *(Expectancy Theory*[3]*,* Vroom 1964) will serve as a basis, justifying certain of these hypotheses.

[3] We will not go into detail regarding the principles stemming from this theory and refer interested readers to the main authors in this field. (Vroom 1964; Connolly 1976; Farag and Krishnan 2003).

CONCEPTUAL FRAMEWORK

The impact of situational factors

Before considering the criteria under evaluation (those corresponding to the perceived attributes), we will begin by specifying the impact of situational factors in our study.

As a general rule, the situational factors likely to have an impact on the consumer's evaluation of data requests can be divided into 3 distinct categories:

- Privacy policies established by a company and/or site;
- The already existing relationship between the company requesting the data and the individual whose information is being requested (e.g. length of prior relationship, satisfaction obtained from previous experiences, etc.);
- The methods used to collect data (anything related to the data entry forms, e.g. elements pertaining to its contents and presentation): the amount and type of data requested the way the questions are formulated, etc.

Out of this set of factors, only a certain number have been thoroughly researched in the past. This is true of privacy policies; the studies examining their influence, however, have almost exclusively been carried out in an American context. It therefore seems of interest to see whether this factor has an equally strong influence in a strictly regulated country such as France. What is more, some researchers recommend a closer examination of the factors linked to the company making the request and its relationship to the consumer from whom it is seeking to obtain data. In this area, most existing work examines the influence of reputation. Yet, according to Zhang, Wang, and Shen (2001), if being a customer of the company requesting the data is not an element that particularly motivates the customer to reply to the data gathering request, *not* being a customer of the company can be a major impediment. In addition to reputation, the individual's prior relationship with a company can therefore have a major impact on the way he/she reacts to the data request. Among these "interpersonal" factors, familiarity with the company — defined both as "the number of product-related (or company-related) experiences that have been accumulated by the consumer" (Alba and Hutchinson 1987, p. 411) and as "the weight of past brand-related (or company-related) experiences" (Siriex and Dubois 1999) — seems likely to have a strong impact, as has already been suggested by the author (2005; 2006).

Finally, among the factors connected with methods of data collecting, and despite it being a topic of some managerial interest, the influence of the amount of data requested has rarely

been studied. Yet this is a factor that a company can easily act on. And although its influence has been the subject of frequent analyses in the context of questionnaire-type surveys, this has not been the case for personal data collection. Moreover, as previous studies concerning the influence of the length of the questionnaire on participation in a survey have proven inconclusive[4], it seems of interest to ascertain whether, in the case of personal information, it is possible to establish a threshold beyond which this hypothesis might be validated.

In summary, the three factors studied in this research are respectively: privacy notices (PN) posted on a website, familiarity with the company requesting the information and the amount of data requested. These factors were chosen both as an attempt to fill the gaps in the literature in this academic field and because of their managerial relevance.

Thanks to research found in the literature review and to the qualitative study carried out beforehand (author 2003), four main perceived attributes of personal data collection can be distinguished: perceived confidentiality, sensitivity and relevance of the data requested, and evaluation of the benefits made available by responding to the data gathering requests (estimation of the cost/benefit ratio). Our research will focus exclusively on the first three dimensions, the fourth being analyzed in another empirical study. The characteristics of each of the dimensions studied here are briefly described in the following paragraphs.

Perceived confidentiality of the data disclosed – This construct corresponds to the "manner in which disclosed data is transmitted and subsequently used." This factor, linked to the consumer's trust that the company will not pass on his personal data to a third party, is crucial. Indeed, once the consumer has disclosed personal data, he/she no longer has any control over its later use (Pavlou and Chellappa 2001). As a result, if there is no guarantee that it will remain confidential, he/she is likely to restrict the amount of data disclosed.

Perceived sensitivity of the requested data – As the literature shows, each piece of information has its own degree of sensitivity, defined by Weible (1993) as the "level of concern experienced by a person for a particular type of data in a specific context." Following in Acquisti's footsteps (2004) however, our study will examine the overall level of sensitivity linked to the types of data requested, so as to be able to compare results.

Perceived relevance of data gathering requests – When faced with a situation where data is being collected, consumers may wonder what motivates the company to engage in data

[4] Although both Kanuk and Berenson (1975) and Heberlein and Baumgartner (1978) show the response rate to be lower for long questionnaires, other studies do not confirm this hypothesis (Roscoe, Lang and Sheth, 1975), and some even go so far as to contradict it (Berdie 1973, Champion and Sear 1969).

gathering and why they are asking so many questions. This is especially the case when the questions asked do not seem related to the transaction being carried out. As a result, data requests considered to lack a proper motive or which are deemed unnecessary in performing this transaction will be viewed by consumers as intrusive, and will often result in a refusal to answer the request, or even, in some cases, in hostility directed towards those requesting the data (Hine and Eve 1998).

This brings us to the underlying hypotheses, starting with the effect of situational factors on perceived attributes (H1) and ending with the impact of these attributes on attitude (H2), the latter being the dependent variable of our model.

The effect of situational factors on perceived attributes

We now present the hypotheses corresponding to H1 and pertaining to the influence[5] of:

- Privacy Notices (PN) on perceived confidentiality and sensitivity (H1.1 a and b[6]),
- Familiarity on perceived confidentiality and relevance[7] (H1.2 a and c),
- Amount on perceived sensitivity and relevance (H1.3 b and c).

Influence of the Privacy notices – Privacy policies address the "expected value" of the Expectancy Theory, i.e. the expectation that an action (such as disclosing data) will result in the expected outcome (here, the data remaining confidential). According to Vroom (1964), the extent to which a company states its practices in formal written policies has an impact on the individual's perceptions. This particularly contributes to his/her trust in the company by allowing him/her to make informed decisions. By posting a privacy policy on their website, e-businesses give clear indications of the type of outcome a customer can expect when disclosing personal data. In addition, announcing their information processing methods and giving the customer the option of controlling the subsequent use of his/her data allows the company to cultivate a relationship of trust with the individual and thus encourages him/her to disclose the requested information (Dinev and Hart, 2002). Culnan and Armstrong (1999)

[5] We have purposely limited the hypotheses related to the influence of the three situational factors on the three perceptual attributes to the six mentioned (out of 9 possible). For one thing, we do not think that the remaining hypotheses are "realistic", and for another, we would not have had the material necessary to justify them.

[6] The names of these hypotheses (the sub hypotheses of H1, such as H1.1 a) are composed of the number assigned to each manipulated factor (e.g. 1 for the "Privacy notice" factor) and of the letter assigned to each mediator variable of the model (e.g. the letter a for "perceived confidentiality") (see figure 1).

[7] Although we did not form a specific hypothesis on the subject, we suspect the existence of possible interaction effects between the manipulated factors. Thus, familiarity could interact coupled with the two other factors (Privacy notices and amount). Chellappa (2001) shows for example that well-known websites are likely to be favored over lesser-known sites, even if the well-known sites have not implemented a privacy policy (few posted notices) thanks to the bond of trust that has already been established between the customer and the company.

specifically show that using ethical practices[8] reduces consumer concern over the confidentiality of data by giving him/her more power and control. Indeed, one of the biggest factors that drive consumers' distrust of e-businesses is the lack of privacy policies. In particular, poorly informed consumers, who are given no choices, will feel as if they have lost control (Culnan, 1995). These overall considerations bring us to the following hypothesis:

Hypothesis 1.1 (a): *The more extensive the privacy notices (PN) are (vs. limited), the higher the confidentiality level of the requested data (vs. low) will be perceived to be.*

When providing data, the consumer pays close attention to the potential consequences of his act (Gandy 1993). As a result, the absence of information regarding the reasons behind the data collection and its consequences (i.e. limited privacy notices) usually leads the consumer to draw his own conclusions, which are most often unfavorable. In addition, because the consumer does not know to what subsequent use his/her data will be put (and cannot control said use), it results in his/her increased vulnerability by diminishing his/her capacity to formulate realistic and appropriate cognitions (Stone and Stone 1990). This then suggests that procedures lacking in transparency lead the consumer to consider the data requested as private and for his/her use alone (which is the strict definition of the concept of data sensitivity). Therefore, the more transparent the data request is perceived to be (thanks to extensive privacy notices), the less invasive the request and the less sensitive the requested data will be perceived to be. This brings us to the following hypothesis:

Hypothesis 1.1 (b): *The more extensive the privacy notices (PN) are (vs. limited), the less sensitive (vs. more) the requested data (b) will be perceived to be.*

Influence of familiarity – Past experience with the company requesting the data seems to be a decisive factor in the willingness to provide information. According to Hine and Eve (1998), whether the data request is perceived as being invasive or not depends on the nature of the relationship between the consumer and the company. Similarly, Culnan and Armstrong (1999) show that relying on an existing relationship ensures that the data gathering request will not be perceived as invasive. Finally, Jourard (1996), as well as Stone and al. (1983) underline that the person to whom the individual self-discloses and the nature of their relationship influence the perceptions of privacy violation. It appears that the consumer's past experiences with the vendor (familiarity) shape his/her evaluation of the risk that disclosing

[8] For example, these can be Fair Information Principles, the ethical principles established in the US by the FTC (Federal Trade Commission).

data represents, particularly relative to confidentiality. Milne and Boza (1999) indicate that past experiences with the company are among the reasons that allow the consumer to trust the company's use of the data disclosed. This brings us to the following hypothesis:

Hypothesis 1.2 (a): *The higher the level of familiarity with the company requesting the data, the higher the level of confidentiality of the data requested (a) will be perceived to be.*

Familiarity also appears to influence the perceived relevance of the data requested. According to Wang and Petrison (1993), consumers will tolerate certain requests, which would be considered by others as invasive and irrelevant, as long as the request comes from a company with which they are familiar. This assessment has been demonstrated many times in the direct marketing field. Rogers (1996), for instance, found that consumers are less hostile to direct marketing operations organized by companies with which they have previously been in contact than to those organized by unfamiliar companies. Applied to data gathering, this brings us to the following hypothesis:

Hypothesis 1.2 (c): *The higher the level of familiarity with the company requesting the data, the higher the level of relevance of the data requested (c) will be perceived to be.*

Influence of amount – The amount of data requested appears to influence the consumer's view of company practices regarding information gathering and subsequent data use. An increase in the amount of data requested seems to lead to a high level of perceived vulnerability. The importance of its impact on cognitions appears to stem from the fact that it not only influences the type of information that could subsequently be inferred about the consumer but also the extent to which disclosing such information could expose the consumer to public censure and the type of action that could then be taken against him (Stone and Stone, 1990). Requesting a large amount of data therefore seems to have an effect on the perceived sensitivity of this data, as is expressed in the following hypothesis:

Hypothesis 1.3 (b): *The more extensive (vs. limited) the amount of data requested (b), the higher (vs. low) the sensitivity of the data will be perceived to be.*

For Woodman and al. (1982), consumers use relevance as a criterion to judge whether a specific item of personal information may be used for a specific purpose. Hence, the greater the amount of data requested, the more the consumer will wonder about the company's real motives in requesting this information, and the more the company therefore runs the risk of

the consumers judging the request to be unrelated to the declared goal. This brings us to the following hypothesis:

Hypothesis 1.3 (c): *The more extensive the amount of data requested (vs. limited), the less relevant (vs. more) the data request (c) will be perceived to be.*

The Effect of Perceived Attributes on Attitude

The effect of evaluating a request for data on attitude can be transformed into hypotheses (H2) relating to the effect of each perceived attribute on attitude.

Influence of confidentiality – Once the data has been provided, the consumer no longer has any control over its use. Consequently, if he/she is not certain the company requesting the data will keep the data confidential, the consumer may choose not to risk self-disclosing (Mayer 2002). Moreover, Moore and McDonald (1987) show that not knowing whether the data will remain confidential — or believing that it will not — contributes to creating an unfavorable opinion. Past studies indicate that when consumers believe that they may be able to control the use of their data, they are less likely to perceive disclosing information as a risk and are therefore more willing to provide data (Culnan and Armstrong 1999; Bies 1993; Stone and Stone 1990). Additionally, the Expectancy Theory posits that control reduces the perceived risk of an action, by increasing the probability that this action will result in the expected outcome. Perceived confidentiality therefore corresponds to the "expected value" aspect of the theory, insofar as a high level of confidentiality leads the individual to think that his/her action will have the expected outcome. This then increases his/her motivation to perform such an action (in this case, providing data). This brings us to the following hypothesis:

Hypothesis 2 (a): *The higher the level of confidentiality of the data requested (a) is perceived to be (vs. low), the more favorable (vs. unfavorable) the attitude toward disclosure will be.*

Influence of sensitivity and relevancy – One important factor in deciding whether to provide information is how sensitive this data is viewed to be (Cranor, Reagle and Ackerman, 1999). Singer (1984) shows that, in surveys, there is a significant link between considering that some questions do not concern the company and non-responsive behavior. Perceived relevance is another important criterion. Several past studies clearly demonstrate its impact on the response process. Hine and Eve (1998) thus observe that any data request that does not result

in an action that benefits the consumer is viewed as intrusive. Hine and Eve (1998) conclude that requests judged irrelevant result in an unfavorable attitude, and in most cases, hostility. Wang and Petrison (1993) corroborate these findings, showing that consumers reject irrelevant actions. Perceived sensitivity and perceived relevance correspond to the "instrumental" aspect of the Expectancy Theory. Indeed, individuals who consider the data requested as too sensitive and/or unrelated to the objective, may not believe that self-disclosure will result in the expected outcome. This tends to reduce their motivation to respond, and therefore brings us to the following hypotheses:

Hypothesis 2 (b): *The higher (vs. low) the sensitivity of the data requested (b) is perceived to be, the less favorable (vs. unfavorable) the attitude toward disclosure will be.*

Hypothesis 2 (c): *The higher the relevance of the data requested (c) is perceived to be (vs. low), the more favorable (vs. unfavorable) the attitude toward disclosure will be.*

The Impact of Privacy Concern

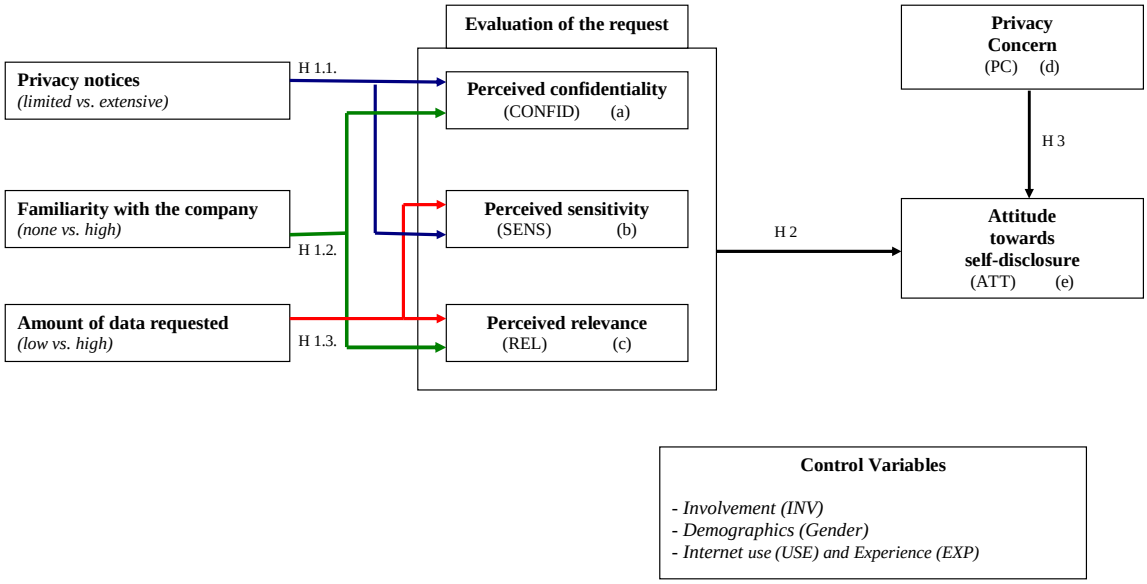
Personal "values" such as privacy concern seem to affect the individual's willingness to communicate his/her personal data, by enhancing the attraction of the expected outcome, i.e. the value the consumer associates with self-disclosure. Hence, the most concerned consumers are likely to perceive the expected outcome as being of lesser value than those who are not particularly concerned. As a result, the former have weaker motivation for self-disclosure. Farag and Krishnan (2003) confirm the fact that privacy concerns may deter the individual from sharing his/her personal information. Their findings show that the most concerned individuals are those who are the most reluctant to share their data for "profiling."

This brings us to our third hypothesis:

Hypothesis 3: *The higher the level of privacy concern (vs. low), the less favorable the attitude towards communicating data (vs. unfavorable) will be.*

The conceptual model for our research can be presented in the following way (see figure 1):

Figure 1. Conceptual model



METHODOLOGY

Experimentation clearly appeared as the most appropriate technique for testing these hypotheses. We first sought to differentiate our research from that already in existence, which favors a survey-based approach poorly suited to evaluating individuals' real-life behavior. The experimental approach, in contrast, allows us to put individuals into a life-like situation — simulated, admittedly, but very similar to real-life experience — and to measure their behavior (here their intended behavior), given the proposed case study. Another virtue of the experimental approach resides in its ability to establish a strong causal relationship between variables (Bagozzi 1977). What is more, it allows a high level of internal validity in testing the model, due to the control exerted over certain variables. In our case study, four exogenous factors likely to influence the response process will be controlled for (see Appendix 1): the respondent's level of involvement (INV) with the category of product/service category[9] offered by the company making the request; his/her gender[10], and finally his/her experience (EXP) and his/her use (USE) of the Internet.

More precisely, two types of controls will be used in this experiment:

- Random assignment of the individuals tested to different treatments (randomization),
- Retrospective statistical control of the set of the exogenous variables identified.

[9] Van Kenhove et al. (2002) indeed show a link between involvement and information decoding

[10] Gender was the only demographic variable controlled for, as the majority of the others (e.g. age, socio-professional group, level of education) were relatively homogenous, due to the specificity of the sample retained (university students).

Experimental Method

The method proposed in the context of this experiment is a 2 x 2 x 2 full-factorial design (8 possible cases in all) for inter-subject comparison (each respondent participating in only one of the 8 possible cases). Hence, the three factors [privacy notices; familiarity; amount] are each manipulated at two levels (limited vs. extensive, none or low vs. high).

Eight different scenarios were thus elaborated in order to create a life-like situation. The experiment consisted of subjecting participants to a simulation exercise where they were asked to provide personal information via the promotional page of a cell phone service provider's website (either their own or an unfamiliar one)[11]. The context of a promotional game is ideal for simulating data gathering, since the situation is both frequently encountered and plausible. The data entry form that needed to be completed in order to take part in the game was then shown to the respondents (See example in Appendix 2). A total of eight different data entry forms were therefore created for this purpose, corresponding to the eight different treatments, with only one shown to each respondent, according to the treatment to which he/she had been assigned.

A privacy notice was included at the end of each data entry form. It either provided little information on the company's privacy policy (requiring the participants to indicate their consent via an opt-out system), or gave a certain amount of information concerning the website's privacy policy (requiring the participants to indicate their consent via an opt-in system[12]), corresponding to both levels of privacy notices (limited [P1] vs. extensive [P2]). The logo of the cell phone service provider conducting the game was displayed at the top of the data entry form. The logo, either that of an unfamiliar company or of their present cell phone service provider, thus corresponds to the two levels of familiarity (none [F1] vs. high [F2]). Lastly, the data entry form proposed was either short (5 fields to complete) or long (20 fields), corresponding to two levels of amount (limited [A1] vs. extensive [A2]).

In summary, the eight treatments selected are presented in the following table (see table 1)

[11] This sector offers the advantage of being at once very involving, of great economic importance and particularly realistic, since the main companies regularly request personal data under various circumstances (for subscription-plan upgrades, when conducting promotional games, when customers join reward programs).

[12] Opting out corresponds to implicit consent, except when explicit refusal is indicated (box to uncheck), whereas opting in, on the contrary, corresponds to explicit consent (generally with a box to check).

Table 1 – Complete Experimental Design

Familiarity (F)				None (1)	High (2)
Amount (A)	Low (1)	Privacy Notices (PN)	Limited (1)	① "P1F1A1"[13]	⑤ "P1F2A1"
			Extensive (2)	② "P2F1A1"	⑥ "P2F2A1"
	High (2)		Limited (1)	③ "P1F1A2"	⑦ "P1F2A2"
			Extensive (2)	④ " P2F1A2"	⑧ "P2F2A2"

Respondent Sample and Questionnaire Administration

The study was carried out on a sample of university students. Such a convenient sample has the advantage to be a homogenous sample. For such a homogenous sample, it is however advisable to make use of factor levels relevant to the sample population (i.e. university students). Choosing an area of activity (cell phone service) and a context of data gathering (i.e. the promotional game) as in our test largely meets this requirement.

After being pre-tested, the questionnaire was administered at random to 5 classes of students (first and second year) enrolled in university Master's programs. Of the 270 completed questionnaires obtained, 27 were "invalidated" for the following reasons: respondent was not a cell phone user, did not use the Internet, questionnaire was incomplete, responses showed a halo effect. Finally, eleven of the 243 remaining questionnaires were eliminated at random to obtain an equal number of participants in each of the treatment groups. We thus obtained 29 participants per treatment, an appropriate sample size according to established procedures[14].

The characteristics of the final 232-participant sample appear in Appendix 3. The overall sample was predominantly female[15] and consisted mainly of experienced Internet users (most participants having 2 to 5 years' prior experience in Web use), although this use was not necessarily on a daily basis (the majority browsed the Web several times a week). Finally, due to their student status and their correspondingly limited financial resources, nearly half of the respondents had never made a purchase on the Internet.

The Validity of the Experimental Design

The validity of the experiment was verified so as to ensure the quality of our findings. Verification consisted of 6 stages, corresponding to the principles governing variance analysis

[13]To be read as follows: P1 for Privacy notice 1 (limited); F1 for familiarity 1 (none) and A1 for amount 1 (low).

[14] It is generally recommended to assign 30 participants per treatment, the minimum at which data distribution is considered normal.

[15] This is no doubt due to the prevalence of female students in the Master's programs from which the respondents were recruited.

(Howell 1998). We have also made sure that the variables were successfully manipulated by verifying that between treatments the mean difference was significant[16].

Operationalizing Variables

The five variables of the model — confidentiality (CONFID), perceived sensitivity (SENS), relevance (REL), privacy concern (PC) and attitude towards personal data requests (ATT) — were subjected to multi-item[17] measures. As no satisfactory scale existed as such for some of these variables, we developed the necessary measuring instruments. The set of items was generated on the basis of verbatim reports drawn from the preliminary qualitative study; those relating to privacy concern included statements from existing scales as well. Five experts then reviewed these sets of items in order to ensure the content validity of the proposed scales. As is standard, the measuring instruments all use the 7-point Likert response format (from "strongly disagree" to "strongly agree").

These multi-item scales were then jointly subjected to quantitative validation procedures on the basis of exploratory analysis (factor analyses in principal components with SPPS 11.5), with confirmatory analysis (measurement model using AMOS 5). As the quality of the scales obtained satisfied the established criteria (Cronbach's α, Jöreskog's ρ, see Appendices 4 and 5), we created other variables by adding the corresponding items.

PRESENTATION AND DISCUSSION OF RESULTS

Overall, in view of the model to be tested, we sought to determine whether:

i) Exposure to data gathering requests (corresponding to the manipulated factors: privacy notices, familiarity and amount) had a real impact on their evaluation (corresponding to the three perceptions tested: perceived confidentiality, sensitivity and relevance).

As previously mentioned, six hypotheses were developed for this purpose: H1.1 (a and b), H1.2 (a and c) and H1.3 (b and c).

ii) An individual, when confronted with the decision to provide personal information, is more likely to base his/her choice on practical considerations (evaluation of the situation) and/or on personal beliefs (particularly his/her level of privacy concern). Four hypotheses come into play here: H2 a, H2 b, H2 c and H3 respectively.

[16] By way of example, the respondents assigned to the "Limited amount" level actually found the questionnaire shorter than those assigned to the "Extensive amount" level (mean scores 1.67 vs. 5.27 respectively; p=0.000).

[17] Involvement (control variable), which will be appraised the three items from the Personal Relevance-Interest-Attraction Scale (Strazzieri 1994), should be added. Here we have retained only one item (out of a possible two) per dimension. This concept consisting initially of only three items, only exploratory analysis will be performed.

The first block of hypotheses will be jointly tested by means of multiple analyses of covariance (MANCOVA) and the second block by means of multiple regression.

Impact of Exposure to Data Requests on the Individual's Attitude

Does the manner in which the data gathering is performed (in terms of privacy notices, familiarity with the company and the amount of data requested) influence the individual's evaluation (in terms of perceived confidentiality, sensitivity and relevance of the data requested)?

The results[18] for variance analysis conducted to answer this question follow:

Table 2 – ANCOVA for the effects of Privacy notices, Familiarity and Amount

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Hypothesis
Corrected Model	CONFID	162.025 (a)	12	13.502	1.729	0.062	
	REL	245.095 (b)	12	20.425	2.435	0.005	
	SENS	381.904 (c)	12	31.825	3.273	0.000	
Constant	CONFID	188.566	1	188.566	24.141	0.000	
	REL	128.846	1	128.846	15.362	0.000	
	SENS	671.273	1	671.273	69.042	0.000	
Involvement	CONFID	22.768	1	22.768	2.915	0.089	
	REL	57.315	1	57.315	6.833	***0.010***	
	SENS	88.729	1	88.729	9.126	***0.003***	
Gender	CONFID	0.104	1	0.104	0.013	0.908	
	REL	1.218	1	1.218	0.145	0.703	
	SENS	3.261	1	3.261	0.335	0.563	
Internet Exp	CONFID	7.183	1	7.183	0.920	0.339	
	REL	7.444	1	7.444	0.887	0.347	
	SENS	14.735	1	14.735	1.516	0.220	
P notices	CONFID	51.305	1	51.305	6.568	***0.011***	***H1.1 a (V)***
	REL	30.774	1	30.774	3.669	***0.057***	
	SENS	33.771	1	33.771	3.473	***0.064***	***H1.1 b (V)***
Familiarity	CONFID	14.230	1	14.230	1.822	0.179	***H1.2 a (NV)***
	REL	1.724	1	1.724	0.206	0.651	***H1.2 c (NV)***
	SENS	19.976	1	19.976	2.055	0.153	
Amount	CONFID	0.006	1	0.006	0.001	0.978	
	REL	80.719	1	80.719	9.624	***0.002***	***H1.3 c (V)***
	SENS	137.903	1	137.903	14.184	***0.000***	***H1.3 b (V)***
Familiarity * Amount	CONFID	23.455	1	23.455	3.003	***0.085***	
	REL	26.085	1	26.085	3.110	***0.079***	
	SENS	22.247	1	22.247	2.288	0.132	
Familiarity * P notices	CONFID	0.007	1	0.007	0.001	0.977	
	REL	9.352	1	9.352	1.115	0.292	
	SENS	3.895	1	3.895	0.401	0.527	

[18] As our hypotheses are formulated with one of the parameters compared greater than the other (H0: m1 – m2>0), we have chosen one-sided tests at 10%. The hypothesis is validated if the significance of the F test for the factor is below 10%. We have maintained the usual 5% threshold for the co-variable effect.

Amount * P notices	CONFID	24.226	1	24.226	3.101	***0.080***	
	REL	0.033	1	0.033	0.004	0.950	
	SENS	19.910	1	19.910	2.048	0.154	
Familiarity * Amount * P notices	CONFID	20.866	1	20.866	2.671	0.104	
	REL	8.474	1	8.474	1.010	0.316	
	SENS	8.718	1	8.718	0.897	0.345	
Error	CONFID	1702.814	218	7.811			
	REL	1828.496	218	8.388			
	SENS	2119.533	218	9.723			
Total	CONFID	17394.000	231				
	REL	14018.410	231				
	SENS	19336.000	231				

(a) $R^2 = 0.087$ (R^2 adjusted = 0.037); (b) $R^2 = 0.118$ (R^2 adjusted = 0.070); (c) $R^2 = 0.153$ (R^2 adjusted = 0.106)

We will first discuss the findings pertaining to the impact of the three manipulated factors[19] (as well as the potential effects of their interactions) before going on to provide a brief description of the influence of the control variables.

The Privacy notices –As we had predicted, Privacy notices have a significant effect on both the perceived confidentiality (p=0.011) and the sensitivity (p=0.064) of the data requested, **thus validating hypotheses H1.1 a and H1.1 b**.

This suggests that the website privacy notices, when posted on the same page as the questionnaire, influence the subject's evaluation of the request for personal data. More specifically, it appears that when extensive Privacy notices are present, the participant has a heightened impression of confidentiality (8.6 vs. 7.8), and a reduced impression of risk in providing his/her personal data (8.2 vs. 8.9) (see Appendix 6).

Posting privacy notices on the questionnaire page appears to help alleviate the individual's concerns about the subsequent use that may be made of his/her personal data (confidentiality) as well as about his/her potential vulnerability as a result of having provided this information (sensitivity). The "Privacy notices" also seem to have a significant impact (an outcome we had not foreseen) on the perceived relevance of the data requested (p=0.057). More specifically, with extensive Privacy notices, the individual appears to perceive the request as being more relevant (7.5 vs. 6.9). Posting Privacy notices, in other words, apparently contributes to reinforcing the company's legitimacy in gathering data. This outcome is of particular interest, in that it had never been suggested in the existing literature.

Familiarity – Contrary to what we assumed, "familiarity" has no (direct) effect on either confidentiality (p=0.179) or the perceived relevance of the data requested (p=0.651); **thus**

[19] The results of multi-varied (Pillai's Trace) tests demonstrate that only the Privacy notices and amount factors have a significant overall impact on the set of perception variables (p=0.048 and p=0.000). Interaction between these two factors is also significant (p=0.058) as is the effect of Involvement (p=0.015).

invalidating hypotheses H1.2 a and H1.2 c. And as we expected, no effect on the data's perceived sensitivity was observed either (p=0.153). Whether an individual's personal data is requested by a company with which he/she is familiar or by one with which he/she has had no prior contact does not appear to impact his/her evaluation of the request, either as concerns confidentiality or the perceived relevance of the data requested. This outcome will no doubt seem surprising, given the literature indicating the contrary. It may however be explained, at least partially, by the effects of interaction. Familiarity, while appearing to have no effect on either confidentiality or relevance, seems to have an impact when combined with the amount of data (p=0.085 and p=0.079 respectively). In other words, when an individual evaluates a data request, he/she will apparently not take familiarity alone into account but rather its interaction with the factor "amount of data requested" (see Appendix 6).

The amount of data – As set out in our hypothesis, "amount" indeed affects the data's perceived sensitivity (p=0.000) and relevance (p=0.002), **thus validating hypotheses H1.3 b and H1.3 c**. As we expected as well, this factor has no observed effect on perceived confidentiality (p=0.978). It does however seem to affect this perception when interacting with the "Privacy notices" factor (p=0.080).

The direct effect of amount on the perception of sensitivity and relevance appears to be in keeping with what we expected (see Appendix 6). Hence, the larger the amount of data requested (long data entry form), the greater the data's sensitivity and the lower its relevance are perceived to be. Findings such as these are easily explained. When the amount of data requested is increased, the level of the individual's impression of vulnerability seems to grow in parallel (high sensitivity), whereas the legitimacy of the company to gather such data is weakened (low relevance). The evaluation of the request appears to become increasingly favorable (in terms of perceived sensitivity and relevance) when the amount of data requested is limited, since this seems to reassure the individual about the intentions of the company gathering the information.

Exogenous variables – Only involvement, of all the exogenous variables tested, has a significant overall impact (p=0.015) on the evaluation of the data request, the impact of the other control variables being either more limited (e.g. Internet use for exchanging messages and browsing) or inexistent (e.g. gender, or prior experience on the Web). More precisely, it seems that the level of involvement reduces the perceived sensitivity and increases the level of perceived relevance (Pearson's correlations = 0.142 and – 0.145; p = 0.05, respectively), with the effect on confidentiality approaching the significance threshold. Both of these

outcomes correspond to what we expected, and confirm the findings of the work on consumer involvement (particularly that of Amine 1990) which state that an involved individual will be more willing to provide information to a company capable of corresponding to his/her expectations and presenting him/her with offers tailored to his/her needs. This criterion (the level of involvement) must therefore be taken into account in evaluating the impact of situation on willingness to provide personal data.

Four of the six hypotheses concerning the manipulated factors' impact on consumers' evaluation of data requests have thus far been validated: **hypotheses H1.1 a, H1.1 b, H1.3 b and H1.3 c,** which stress the importance of Privacy notices and the amount of data requested.

We will now present our findings concerning the impact of data gathering request evaluations and privacy concern on consumer attitude toward providing personal data.

The Impact of Evaluation and Privacy Concern on Providing Personal Data

Here we test our model's core assumptions: that is, the impact of situation (evaluation) and of individual characteristics (privacy concern) respectively, on the individual's degree of approval regarding the disclosure of his/her personal information (attitude). Our objective is therefore to ascertain:

i) Whether the two "mechanisms" combine to influence attitude;

ii) What the respective effects of situational and individual characteristics are.

The results of regression analysis performed to reply to these two queries are the following:

Table 3 –Attitude toward providing data

	Model 1		Model 2		Model 3		Collinearity	
	B	Sig.	B	Sig.	B	Sig.	Tol.	VIF
Constant	8.918	0.000	13.175	0.000	13.745	0.000		
PerceivedConfidentiality	0.291	***0.003***	0.202	***0.042***	0.192	***0.054***	0.761	1.314
Perceived Sensitivity	- 0.361	***0.000***	- 0.313	***0.001***	- 0.308	***0.001***	0.607	1.647
Perceived Relevance	0.485	***0.000***	0.377	***0.001***	0.346	***0.002***	0.546	1.830
Privacy Concern			-0.220	***0.001***	- 0.233	***0.000***	0.656	1.523
Involvement					0.111	0.086	0.923	1.084
Gender					- 0.127	0.808	0.962	1.040
Internet Experience					- 0.078	0.852	0.939	1.064
E-mail					- 0.113	0.598	0.922	1.085
Web Browsing					- 0.225	0.433	0.838	1.194
R^2	0.354		0.386		0.399		-	
R^2 Adjusted	0.346		0.375		0.374		-	

These results demonstrate the significance of the three perception variables' (confidentiality, sensitivity and relevance) influence on attitude toward providing personal data, even after the second and third blocks (p=0.054 p=0.001; and p=0.002 respectively) are introduced, thus **proving hypotheses H2 a, H2 b and H2 c to be valid.** Hence, as we assumed, the evaluation of the data request (perceptions) significantly influences the individual's attitude toward revealing personal data. Moreover, this "situational" influence[20] has proven to be of major importance, as it explains almost 35% of the model's variance. Among the perception variables, sensitivity and relevance appear to be the decisive elements and better account for attitude than perceived confidentiality[21].

The influence of privacy concern (individual variable) is shown to be significant as well (p=0.000), although its introduction does not significantly enhance the explanatory power of the model (37.4% with vs. 34.6% without, or a gain of less than 3%). **Hypothesis H3 is thus validated**, as it posited the variable's effect on consumer attitude toward providing personal data. What is more, examining standardized coefficients shows that concern has a stronger influence on attitude than confidentiality and an influence quasi equal to that of perceived sensitivity and relevance (beta = - 0.229). Finally, introducing control variables does not enhance the explanatory power of the model either, as none of these variables prove to be significant beyond the 5% threshold. Involvement alone influences attitude; the coefficient, however, is only significant at the 10% threshold.

Finally, the four **hypotheses tested here were validated** (**H2 a, H2 b, H2 c and H3)**, thus emphasizing the impact of the three perception variables and of privacy concern on attitude toward data requests. The influence of situation (through the three perceptions) would however appear to be significantly greater than that linked to individual characteristics (through privacy concern), the latter accounting for 3% of the model as opposed to 35% for the situational characteristics. These findings indicate that, when confronted with a data request, there is a greater likelihood that an individual will base his/her decision on the situation in which he/she finds him/herself rather than on personal convictions. This confirms the findings of Acquisti (2004) and Acquisti and Grossklags (2004), which show the existence of a discrepancy between the individual's general attitude toward privacy concern and his/her decision when data is actually requested. Hence, an individual who is extremely concerned about his/her privacy might accept to part with personal information if the context in which

[20] As opposed to individual influence linked to individuals' personal characteristics.

[21] This information is drawn from the standardized coefficient (beta) readings of 0.116 (for confidentiality); 0.220 (for relevance) and - 0.215 (for sensitivity) respectively.

he/she finds him/herself offers safeguards and is highly reassuring (high confidentiality and perceived relevance; low sensitivity of data requests), and vice versa.

In conclusion, we have demonstrated the existence of a response process that begins with the data gathering request, continues through the evaluation of the situation (in the form of perception attributes), and ends with the data being provided. We have also proven that situation (at least the Privacy notices and the amount of data) and individual factors (via privacy concern) significantly influence the willingness to disclose personal data.

CONTRIBUTIONS, LIMITATIONS AND FURTHER AVENUES OF RESEARCH

Study Contributions

Our research seeks to make a contribution not only to the academic literature but also to managerial practice. From the academic standpoint, our study contributes to knowledge about the impact of privacy concern on self-disclosure, particularly on the Internet. The results of this research, confronted with work resulting from the literature, thus enable us to enrich comprehension of the consumer decision-making process. This work allowed the development of a conceptual model aiming at explaining the way in which a consumer solicited to provide personal information apprehends the phenomenon. The innovative character of this model lies partly in the choice of a "processual" vision of the answering process, approach largely been unaware of in the literature. We also privileged a "realistic" approach of the phenomenon, while seeking to put the people in a situation which as much as possible approaches the real conditions of a request of personal data on Internet. The model has, moreover, the advantage of including at the same time situational factors (corresponding to the exposure to the request) and individual characteristics (in particular through the concern for privacy), and thus of being able to test the respective impact of each one of them. We chose factors largely ignored up to now in existing research and with strong managerial importance. Lastly, our results clearly show the influence of individual and situational factors on attitude toward data disclosure, with the influence of the latter being predominant, a fact that had never been empirically demonstrated in previous work.

Several implications of managerial relevance are also to be underlined. Our results should encourage managers to pay more attention to the manner in which they request data from their customers and, in particular, to the Privacy notices and the amount of information requested in the data entry form. It indeed appears that posting Privacy notices will increase the individual's willingness to disclose information by making the data more confidential, and the information disclosed, less sensitive.

Websites should therefore make their privacy policies highly visible, particularly on the pages containing data entry forms, so as to reassure consumers with privacy concerns. Similarly, a long data entry form — which technically allows a company to obtain in-depth knowledge of consumers — may well turn out to be counter-productive, because it could in fact discourage individuals from self-disclosure. The company should therefore keep a sense of proportionality between data entry forms and the context in which questions are asked, and in consequence, restrict the data requested to fully relevant items. And, although familiarity may not have a direct effect on the perception variables tested here, it however seems to influence both the degree of confidentiality and the relevance of the data requested, when coupled with the amount. This is therefore an element to be reckoned with. Finally, even if the effect of privacy concern has turned out to be of less importance than that of situational variables, it should not be deduced that a respondent is any less desirous of being kept informed and reassured about the subsequent use of his/her personal data. And although privacy concern may not have a major impact on the decision whether to complete data entry forms, its impact is by no means negligible; moreover, it could also explain other behaviors such as disclosing sensitive information and lying.

Limitations and Suggestions for Further Research

As is the case with all empirical research, ours is not without limitations.

First of all, only three of the situational factors likely to influence the responses to data gathering requests were studied. Our findings are also dependent on the manner in which the factors selected were operationalized. For instance, we chose to operationalize privacy policies by using the Privacy notices included in data entry forms. We could, of course, have simply limited ourselves to studying the presence or absence of a code of conduct on the site, as most researchers have done. However, as Sprott, Hardesty and Miyazaki (1998) point out, the format chosen to operationalize the Privacy notices can influence the consumers' perceptions and therefore alter the outcome. Further research will therefore be necessary to test the impact of other Privacy notice formats, so as to determine their real impact whatever the format used. The approach chosen here to operationalize familiarity may also have affected our findings. Future studies should thus be conducted not only in order to manipulate other factors, but also to operationalize the factors tested here in a different manner.

Second, our respondents were questioned using paper-and-pencil questionnaires. This type of simulation is not necessarily the most appropriate method to gain insight into the subject and it may thus be preferable to consider using a more realistic design. The idea of questioning the

respondents via an online questionnaire would be one possible approach, which could subsequently be improved by putting respondents into a life-like situation.

The third limitation is linked to the sample type and to the context of the simulation exercise. Indeed, during this experiment, we questioned a homogeneous sample population — students — following a specific scenario (a promotional game organized by a cell phone service provider). The choice of the context in itself limits the generalizability of our findings. This type of data request is in fact very specific, and the same individuals would likely react in a different manner in other cases (other sector, other context). What is more, convenience samples (particularly when composed of students) do not (always) provide an appropriate context to obtain behavior patterns representative of the population as a whole. Further research is therefore necessary in order to confirm that the validity of the results obtained here may be generalized, by focusing on a more representative sample. Finally, work extrapolating our findings to business sectors other than cell phones and to other media (aside from the Internet) would be most welcome.

Appendix A — Control Variables Measurement

Variables	Items	Scale Format
Involvement level	Scale adapted from the literature [Strazzieri (1994)] Simplified version (3 items)	Likert (7 points) (from 1 “strongly disagree” to 7 “strongly agree”)
Gender	M / F (1 item)	Binary variable
Internet experience	Has used the Internet for less than 2 years/ between 2 and 5 years/ more than 5 years (1 item)	Ordinal variable 3 levels
Internet use	Checks Email account and browses the Web (2 items): more than once a day, once a day, more than once a week, less often (1 item)	Ordinal variables 4 levels

Appendix B — Sample Screenshots Corresponding to Data Entry Forms

P1F1A1 ("limited" Privacy notices, none Familiarity, low Amount)

Logo of an unknown cell phone supplier

Take part in the Lottery and win $5,000!

Just fill out the following form:
(* required information)

Name*: _____
Address*: _____
City*: _____ Zip Code*: _____
Email Address*: _____@_____

I wish to receive offers by Email ☐ YES ☐ NO

I wish to receive offers from partner companies ☐ YES ☐ NO

P2F2A2 ("extensive" Privacy notices, high Familiarity, high Amount)

Logo of the respondent's cell phone supplier

Take part in the Lottery and win $5,000!

Just fill out the following form:
(* required information)

Title *: _____
Last Name *: _____ First Name *: _____
Address *: _____
City*: _____ Zip Code*: _____
Email Address *: _____@_____
Phone Number *: _____
Country *: _____
Birth Date: _____
Education *: _____
Profession *: _____
Marital Status *: _____ Number of children: _____
Hobbies *: _____
Time spent phoning *: _____
Cell phone date of purchase *: _____
Use of SMS and MMS *: _____
To sponsor a friend, indicate his/her email address here*:
_____@_____
Yearly income: _____

This information is for company use only. It will help us to provide you with the very best in service and useful information. Your personal information will not be passed on to third parties without your consent. To learn more about our privacy policy, please click here

I wish to receive offers by Email ☐ YES ☑ NO

I wish to receive offers from partner companies ☐ YES ☑ NO

Appendix C — Sample Characteristics

Variables	Values	Frequency	%
Demographics			
Gender	M	85	36.6%
	F	147	63.4%
Experience			
Internet experience	Less than 2 years	17	7.3%
	Between 2 and 5 years	120	51.7%
	More than 5 years	95	40.9%
Email use	More than once a day	27	13.0%
	Once a day	54	26.0%
	More than once a week	87	41.8%
	Less often	40	19.2%
Web use	More than once a day	29	12.5%
	Once a day	35	15.1%
	More than once a week	110	47.4%
	Less often	58	25.0%
Online purchase history	None	111	47.8%
	Less than 5	63	27.2%
	5 to 20	45	19.4%
	More than 20	13	5.6%

Appendix D — Results of Exploratory Factor Analysis (EFA)

Variables	Items before EFA	Items after EFA	KMO/ Bartlett Test	Percentage of Variance	Loadings min	Loadings max	Cronbach's α
Perceived confidentiality	4	3	0.669/0.000	67.5%	0.58	0.72	0.74
Perceived sensitivity	5	3	0.651/0.000	72.7%	0.56	0.81	0.80
Perceived relevance	4	3	0.772/0.000	70.5%	0.63	0.77	0.79
Privacy concern	4	3	0.729/0.000	77.2%	0.74	0.79	0.85
Attitude	4	3	0.723/0.000	77.0%	0.75	0.81	0.85
Involvement	3	3	0.682/0.000	66.2%	0.61	0.70	0.74

Appendix E — Results of Confirmatory Factor Analysis (CFA)

Variables	Items	Reliability		Convergent Validity (ρvc)	Discriminant Validity	Predictive Validity
		α	Rhô			
Perceived confidentiality	2	0.77	0.795	0.660	yes	yes
Perceived sensitivity	2	0.78	0.796	0.661	yes	yes
Perceived relevance	2	0.83	0.773	0.630	yes	yes
Privacy concern	3	0.87	0.876	0.702	yes	yes
Attitude	3	0.81	0.836	0.634	yes	yes
Involvement	3	0.82	-	-	-	-

Appendix F — Effect of Manipulations on Perceptions

Figure 1. Effect of Privacy notices on perceived confidentiality and sensitivity

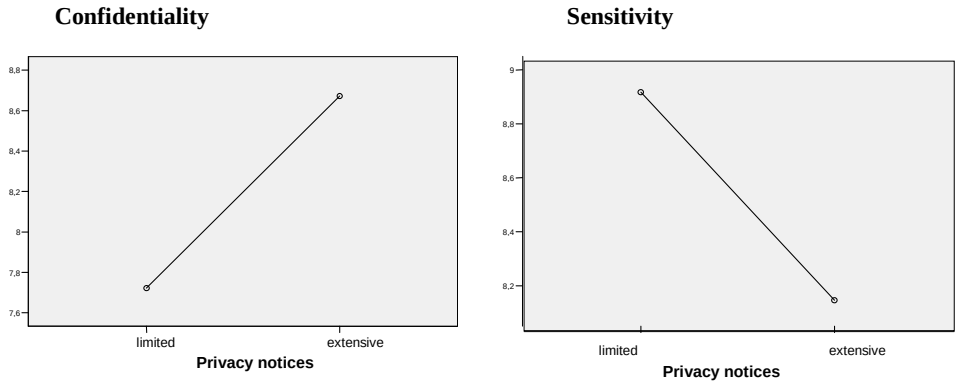


Figure 2. Effects of Familiarity x Amount on perceived confidentiality and relevance

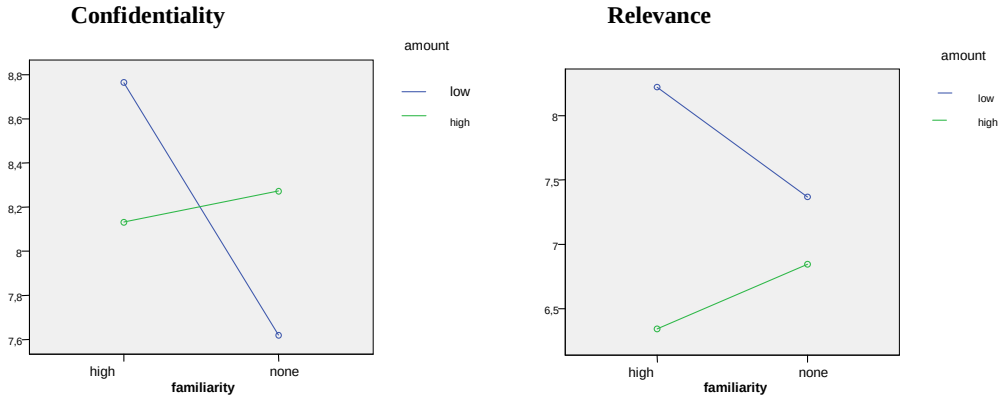
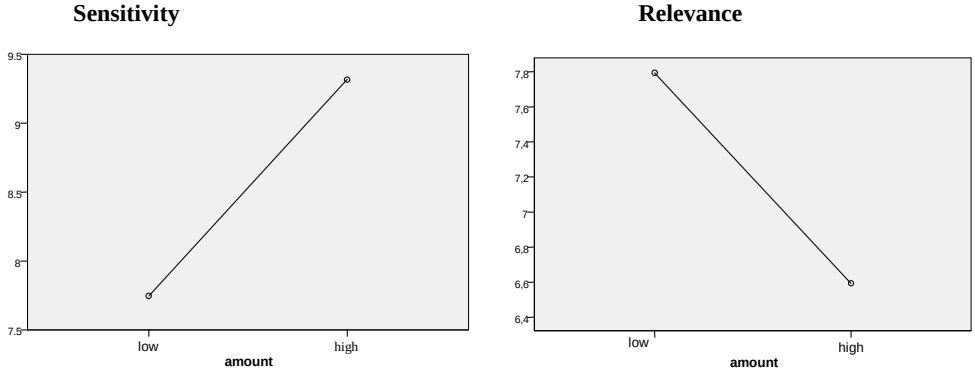


Figure 3. Effects of Amount on perceived sensitivity and relevance



REFERENCES

Author (2005) ; (2006)

Acquisti A. (2004), Privacy in electronic commerce and the economics of immediate gratification, *Electronic Commerce Conference*, New York, USA, May

Acquisti A. and Grossklags J. (2004), Privacy and rationality: evidence from survey data, *Workshop on Economics and Information Security*

Alba J. and Hutchinson J. (1987), Dimensions of consumer expertise, *Journal of Consumer Research*, 13, 411-454

Amine A. (1990), Comparative test of two involvement measurement scales [Essai comparatif de deux échelles de mesure de l'implication], *International Congress, Association Française du Marketing*, La Baule, 512-539

Bagozzi R. (1977), Structural equation models in experimental research, *Journal of Marketing Research*, 14, 209-226

Beauvois J.-L. and Joule R. (1981*), Submission and ideologies : the social psychology of the rationalization [Soumission et Idéologies : Psychosociologie de la Rationalisation]*, Presses Universitaires de France, Paris

Berdie D. (1973), Questionnaire length and response rate, *Journal of Applied Psychology*, 58 (October), 278-280

Calder B., Phillips L. and Tybout A. (1983), Beyond external validity, *Journal of Consumer Research*, 10, 112-114

Champion D. and Sear A. (1969), Questionnaire response rate : a methodological analysis, *Social Forces*, 47, 335-339

Chellappa R. (2001), Contrasting expert assessment of privacy with perceived privacy: implications for public policy, www.ebizlab.usc.edu

Connolly T. (1976), Some conceptual and methodological issues in expectancy models of work performance motivation, *Academy of Management Review*, 179-186

Cranor L., Reagle J. and Ackerman M. (1999), Beyond concern: understanding net users' attitudes about online privacy, AT&T Labs, Research Technical Report, 99.4.3

Culnan M. (1995), Consumer awareness of name removal procedures: implications for direct marketing, *Journal of Direct Marketing*, 9, 2, 10-19

Culnan M. and Armstrong P. (1999), Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation, *Organization Science*, 10, 1, 104-115

Dinev T. and Hart P. (2002), Internet privacy concerns and trade-off factors: empirical study and business implications, *International Conference On Advances In Infrastructure for E-Business*, L'Aquila, Italy

Dommeyer C. and Gross B. (2003), What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies, *Journal of Interactive Marketing*, 17, 2, 34-51

Farag N. and Krishnan M. (2003), An empirical evaluation of information features and the willingness to be profiled online for personalization, online, http://misrc.umn.edu/workshops/2003/spring/farag_030703.pdf

Fishbein M. and Ajzen I. (1975), *Belief, attitude, intention and behaviour: An introduction to theory and research*, Reading, Mass.: Addison-Wesley

Gandy O. (1993), *The Panoptic Sort: A Political Economy of Personal Information*, Boulder: Westview Press.

Heberlein T. and Baumgartner R. (1978), Factors affecting response rates to mailed questionnaires: a quantitative analysis of the published literature, *American Sociological Review*, 43, 4, 447-462

Hine C. and Eve J. (1998), Privacy in the marketplace, *The Information Society*, 14, 253-262

Howell D. (1998), *Méthodes Statistiques en Sciences Humaines*, DeBoeck Université, Paris

Jourard S. (1966), Some psychological aspects of privacy, *Law and Contemporary Problems*, 31, 307-318

Kanuk L. and Berenson C. (1975), Mail surveys and response rates: a literature review, *Journal of Marketing Research*, 12, November, 440-453

Mayer T. (2002), Privacy and confidentiality research and the U.S. Census Bureau: recommendations based on a review of the literature, Research Report Series, February

Milne G. and Boza M. (1999), Trust and concern in consumers' perceptions of marketing information management practices, *Journal of interactive Marketing*, 13, 1, 5-24

Moore J. and McDonald S. (1987), The Census community awareness program : an evaluation of the potential and actual effectiveness of CCAP based on evidence from the 1986 Los Angeles Census test, Report prepared for the bureau of the Census, February

Olson J. and Dover P. (1978), Cognitive effects of deceptive advertising, *Journal of Marketing Research*, 15, February, 29-38

Pavlou P. and Chellappa R. (2001), The role of perceived privacy and perceived security in the development of trust in electronic commerce transaction, *ISR*

Phelps J., Nowak G. and Ferrell E. (2000), Privacy concerns and consumer willingness to provide personal Information, *Journal of Public Policy & Marketing*, 19, 1, 27-41

Rogers J. (1996), Mail advertising and consumer behaviour, *Psychology and Marketing*, 13, 2, 211-233

Roscoe A., Lang D. and Sheth J. (1975), Follow-up methods, questionnaire length and market differences in mail surveys, *Journal of Marketing*, 39, April, 20-27

Singer E. (1984), Public reactions to some ethical issues of social research: attitudes and behaviour, Journal of Consumer Research, 11, 501-509

Siriex L. and Dubois P.-L. (1999), Toward a quality-satisfaction model integrating trust [Vers un modèle qualité satisfaction intégrant la confiance, *Recherche et Applications en Marketing*, 14, 3, 1-22

Sprott D., Hardesty D. and Miyazaki A. (1998), Disclosure of odds information: an empirical investigation of objective odds format and numeric complexity, *Journal of Public Policy and Marketing*, 17, 1, 11-23

Stone E., Gueutal H., Gardener D. and McClure S. (1983), A field experiment comparing information privacy values, beliefs and attitudes across several types of organizations, *Journal of Applied Psychology*, 68, 3, 459-468

Stone E. and Stone D. (1990), Privacy in organizations: theoretical issues, research findings and protection mechanisms, *Research in Personnel and Human Resources Management*, 8, 349-411

Strazzieri A. (1994), Measuring involvement without perceived risk [Mesurer l'implication durable vis-à-vis d'un produit indépendamment du risque perçu], *Recherche et Applications en Marketing*, 9, 1, 73-92.

Van Kenhove P., Wijnen K. and De Wulf K. (2002), The influence of topic involvement on mail survey response behaviour, *Psychology and Marketing*, 19, 3, 293-301

Vroom V. (1964), *Work and Motivation*, New York: Wiley

Wang P. and Petrison L. (1993), Direct marketing activities and personal privacy, *Journal of Direct Marketing*, 7, 1, 7-19

Warren S. and Brandeis L. (1890), The right to privacy, *Harvard Law Review*, 4, 5

Weible R. (1993), Privacy and data: an empirical study of the influence of types of data and situational context upon privacy perceptions, Doctoral Dissertation

Westin A. (1967), *Privacy and Freedom*, New York: Atheneum

Woodman R. et al. (1982), A survey of employee perceptions of information privacy in organizations, *Academy of Management Journal*, 25, 3, 647-663

Zhang Y., Wang C. and Chen J. (2001), Chinese online consumers' responses to web-based data collection efforts: a comparison with American online consumers, *Journal of Database Marketing*, 8, 4, 360-369