A Study of the Major Factors Influencing the Perception Consumers Have about How their Privacy Is Being Invaded while Surfing the Net

Jacques Nantel*, Cristiana Élie ‡

* HEC – Montreal
Department of marketing
Montreal, Quebec, Canada
Jacques Nantel@hec.ca

‡ HEC – Montreal
Graduate student
Montreal, Quebec, Canada
cristiana.elie@hec.ca

Abstract

The topic of privacy on the web is becoming an issue of key importance. Although several studies have been conducted in order to assess the degree to which privacy is a major concern for consumers and whether it can prevent them from buying on the web, we still lack a good understanding of what consumers mean by privacy and private life on the net.

The study was performed using an in-between factorial experimental design. A total of 120 consumers were asked to evaluate one of 12 scenarios which described various combinations of private information usage/ marketing strategy. Result demonstrate that while consumers do tolerate some invasion to their privacy, especially if those contribute positively to their well-being, they react very negatively to some of the most pervasive marketing strategies.

Keywords Consumer behaviors, trust, internet, experiment, privacy

1. INTRODUCTION

Today, consumers realize that companies use information concerning them to create targeted marketing campaigns (Culnan and Armstrong, 1999; Novak et al., 1998). Yet the fact that consumers do not necessarily know the way in which marketing managers have acquired this information or the way they plan to reuse it has transformed this general understanding into a lack of trust in marketing managers' respect for consumers' privacy (Glickman, 2000). This lack of confidence or trust is even more pronounced on the Internet, given the ease of gathering information compared with traditional methods (Novak et al., 1998). The Internet allows the generation and updating of information in real time, directly at the time of the transaction, along with automatic transfers to a database that contains the consumer profile (Caudill and Murphy, 2000; Sheehan and Hoy, 2000). This data can then be cross-referenced with other bases accessible on the market, at a relatively low cost (Prabhaker, 2000).

Techniques such as "cookies," registration or contest entry forms, managing personalized online advertising banners (Charters 2002) and universal identification services enable Internet sites to collect data regarding consumer behavior that is more precise than that acquired through traditional methods. This data can subsequently be used to assign a singular profile to a consumer and to target consumers individually (Caudill and Murphy, 2000; Prabhaker, 2000). Paradoxically, the same technological advances that have propelled companies to new peaks of competitiveness have concomitantly introduced risks of invasion of consumer privacy (Nowak and Phelps, 1992; Peppers and Rogers, 1993). Accordingly, numerous studies conducted in the past decade have revealed that consumers are quite suspicious of companies' possessing information about them, of how the companies obtain and use this information, and the precision of the information used (Cranor et al., 1999; Culnan, 1993, 1999;). If the research largely demonstrates that consumers show a marked interest in the use that companies make of data concerning them, other studies conclude that consumers are nonetheless willing to supply information in return for personal benefits (Goodwin, 1991; Milne, Boza and Rohm 1999;

Sheehan and Hoy, 1999; Milne and Rohm, 2000; Sheehan and Hoy, 2000). Various studies have investigated the sources of consumers' concerns regarding their privacy (Milne and Boza, 1999; Nowak and Phelps, 1997; Sheehan and Hoy, 2000). Both the data collection method and the reasons and marketing strategies associated with reuse have been studied extensively (Goodwin, 1991; Milne and Boza, 1999; Phelps et al., 2000). Although this diverse body of research has evinced consumers' degree of tolerance regarding collection, use and reuse of private data, most of the studies are marred by the shortcoming of using a survey to measure the degree of consumer tolerance of various marketing practices. Indeed, too often these evaluations of marketing practices are performed out of context, and practices are examined singly. The researchers thus overlook the possibility that consumers may be willing to have certain data resold to a third party. Consumers may also be receptive to receiving email from a company with which they transact even if they consider that this email is unrelated to the initial transaction. However, consumers' limit of tolerance may be exceeded if they receive an unsolicited email from a company they do not know. Assuming that the tolerance threshold of consumers regarding invasion of privacy is not a function of practices taken individually but rather of a combination of these practices, we have performed a study founded on an experimental design that investigates the impact on consumer confidence of various marketing practices, along with their interactive effects.

2. PROTECTION OF CONSUMERS' PRIVACY

Alan Westin (1967) defines the concept of privacy as follows:

> "*[…] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"* (Westin, 1967, p. 7).

Westin's (1967) definition thus refers to the informational aspect of privacy. Because information regarding an individual, group or even organization can be gathered and disclosed without their knowledge or even their consent, privacy with regard to information goes beyond personal control (Burgoon, 1982). In recent years the problem of ensuring respect for privacy has intensified owing to the abundant quantity of information gathered on individuals, along with the growing ease of collection, management and reuse of this information, fuelled by technological advances. Burgoon (1982) asserts that the real threat to privacy posed by these new technologies, in particular the Internet, is linked to several factors.

The first factor is the degree of control that individuals can exercise, not only over initial disclosure of information, but also over its transmission and *a posteriori* use. Most individuals do not object to supplying personal information of a public nature, such as their marital status and occupation, when required by a form, for example.

The second factor is the quantity of information possessed by others. If an individual has the impression that the quantity of their personal information possessed by others is minimal, then their perceived vulnerability to invasion of privacy will decrease. Many Internet users are convinced that the quantity of their personal information available is minimal because they did not supply it directly (Caudill and Murphy, 2000; Cranor et al., 1999; Miyazaki and Fernandez, 2001). However, Internet users are becoming increasingly aware that Internet sites possess considerable information regarding them without their having had to supply it directly, and without their having provided their consent. This awareness has spawned growing concern among Internet users.

Closely linked to the second factor, the third factor is the number of people who have access to the information. Even the most commonplace information, distributed to too many people, may create a significant feeling of worry regarding its further dissemination and abuse.

The fourth factor is the information type factor. The more personal the information, the more vulnerable the individual becomes regarding the power and influence that others can wield over them if this information is made public. In addition, the types of information that individuals are more reticent to supply also seem to be those that which create the strongest feeling of invasion of privacy. This point will be explored in greater detail in the definition of personal information.

The final factor refers to the nature of the relation with the entity that possesses the information. Recent technological advances have significantly increased the likelihood that an individual will never be aware of the identity of the organization that is gathering information regarding them. Moreover, knowing the identity of the entity that possesses the information does not imply knowing the entity that will reuse this information. Therefore, consumers are gradually noting that the entities that compile information regarding them are not necessarily those that initially gathered it.

On the Internet, a relationship exchange (or transaction) entails not only a monetary exchange between two entities, but also exchanges that are often indirect, which may include intangible and symbolic aspect, and in which more than two parties may participate (Novak et al., 1997). To initiate a relationship exchange, trust is a necessary condition. Because the Internet contains a substantial quantity of information gathered without consumers' consent, we can therefore assert that a violation of this trust between the consumer and the company occurs more often than in the traditional physical context. Novak et al. (1998) affirm that "*consumers simply do not trust most Web providers enough to engage in "relationship exchanges" involving money and personal information."* In addition, an Internet study conducted by Arthur Andersen/Andersen Legal (2000, cited in Ang, Dubelaar and Lee, 2001) found that the fear of the misuse of personal information disclosed is cited most often by Internet users' as the main reason for their lack of trust in a site.

Apparently, 92% of consumers are worried and 67% are very worried about improper use of personal information by Internet sites (Louis Harris & Associates, 1999). In addition, 76% of consumers that were not worried about the use of personal information in a traditional context were worried in an Internet context. This concern has a direct impact on sales conducted on the Internet. One study (Forrester Privacy Best Practice Report, 2000, cited in FTC, 2000) estimates that worries regarding privacy account for roughly $2.8 billion in lost online sales in 1999, whereas another study (Junnarkar, 1999, cited in FTC, 2000) suggests that the probable losses in online sales may reach $18 billion (compared with projected sales of $40 billion) by 2002 if measures are not taken to allay these worries. In addition, consumers' level of concern was highlighted by Odyssey (2000, cited in FTC, 2000), which found that 92% of respondents with Internet service at home reported that they do not trust companies to preserve confidential information, and 82% of respondents believe that the government should legislate the use of personal information by companies.

The link between the importance that consumers place on having their privacy preserved and the trust placed in an Internet site, in particular a commercial site, has been studied extensively. Rohm and Milne (1998), and Sheehan and Hoy (2000) advance that most Internet users are worried about the collection of information by Internet sites in general, regardless of whether they make online purchases. In addition, the more Internet users perceive a lack of control regarding the collection of personal information, the lesser their feeling of trust in a site (Novak et al., 1998). In contrast, trust is created when an Internet site is able to reassure users of favorable exchange conditions, such as the type of information that they want to collect, for which reasons and the way the information will be reused (Glickman, 2000).

3. THREATS TO PERCEPTION ON CONTROL OVER PRIVACY

Some of the marketing practices that prevail on the Internet, and especially certain combinations of these practices, pose a threat to consumer privacy. Such practices may thus erode consumers' trust in companies that use them. This study will examine four of these contentious practices.

3.1 Data collection methods

In general, data is collected covertly, without the knowledge or consent of the Internet user, by means of "cookies," or the extraction of email addresses from lists of servers, chat rooms and discussion forums (Caudill and Murphy, 2000). Alternately, it is collected overtly, by asking the Internet user directly for the information as part of the registration form. We believe that the relation of trust may be adversely affected by collection mechanisms that Internet sites use. The gathering of information by an explicit form is commonplace on many Internet sites, in this case the relation of trust between consumers and the site regarding respect for privacy is not undermined to the same extent because the consumers supply information willingly (Nowak and Phelps, 1997). In contrast, studies of the use of numerous sites of "cookies"

demonstrates that 52% of consumers report that they are worried about these “cookies,” whereas 12% claim that they are uncertain, even confused about their actual definition (Cranor et al., 1999). For instance, some respondents believe that "cookies" are able to create information that can personally identify them and automatically send this information to other Internet sites. or that “cookies” can reveal their identity following navigation to any site.

3.2 Information usage mode

Several researchers have identified that consumers’ worries regarding the reuse of information on the Internet are mainly translated by the fear of the sale of personal information by an Internet site to a third party, without their knowledge or their permission. It is mainly this aspect, described above, which influences Internet users’ feeling of confidence in an Internet site’s respect for their privacy. One study indicated that 69% of respondents consider it important or very important to mention the purpose of data collection (Cranor et al., 1999). Internet users’ attitude toward the reuse of information by Internet sites may thus have positive and negative impacts for the company depending on the entity that reuses the data and the way in which the information is reused (Culnan and Armstrong, 1999).

A primary concern regarding the reuse of information relates to the entity that reuses this information. We can thus distinguish between a use made by an entity that initially gathered the information (internal reuse) and that by a third party to which the information was exchanged or sold (external reuse) (Culnan, 1993; Smith et al., 1996; Wang et al., 1998). Because internal reuse implies that the information gathered is used by the same entity that collected it, the feeling of confidence regarding respect for privacy is not as negatively influenced as in the case of external reuse.

3.3 Pertinence of use of information

In both cases, whether it is the same entity that gathered the information or another entity, reuse may be either pertinent or non-pertinent. In the first case, the reuse of the information is directly linked to the initial transaction that generated the collection (pertinent reuse). In the second case, the purpose of the reuse has no relation to the initial transaction (non-pertinent reuse). Whereas pertinent reuse of information gathered does not appear to create a negative feeling toward the company that uses the information, non-pertinent reuse negatively affects the consumers’ feeling of trust in an organization.

3.4 Marketing strategy adopted

For this study, we have retained two marketing strategies that are currently used by Internet sites to justify the collection of information from Internet users. The first strategy is that of personalized advertising, the second consists of email (associated with permission marketing).

One of the main advantages of the Internet is the capacity to produce personalized advertising messages. This type of advertisement contains a message directly adapted to the preferences or tastes previously specified by Internet users (Lombard and Snyder-Duch, 2001; Fitzgerald, 1999). To engage in personalized advertising, advertisers require information regarding the target customers.

In contrast, the transmission of email by an Internet site sends often rests on the principle of “permission marketing,” whereby consumers are encouraged to participate in an interactive and enduring marketing campaign that rewards the attention visitors pay to increasingly better adapted messages (Godin, 1999). Permission marketing is underpinned by a personalized relation and generally includes three characteristics: the message is expected, personalized and pertinent. Ultimately, for a permission marketing strategy to be effective, consumers must have confidence in the site that asks for their email address (Culnan and Armstrong, 1999; Godin, 1999).

3.5 Moderating variables

Because the sensitivity to invasion of privacy varies between consumers, the relation of trust between consumers and companies that engage in information-based marketing presumably varies as well. Therefore, two variables are considered in this study: the structural predisposition to transmit information and the attitude toward reuse of the information. Cranor (1999) showed that consumers' predisposition to feel that their privacy is being invaded by some web sites influences their confidence in various sites. The same phenomenon was seen in consumers' attitude toward the reuse of this information (Sheehan and Hoy, 2000).

4. RESEARCH HYPOTHESES

As the literature largely demonstrates that the way in which a company gathers information on consumers has an impact on their degree of trust, we formulate our first hypothesis as follows.

> ***H_1:*** *The use of a form generates a greater feeling of trust than the use of "cookies."*

Similarly, as the literature suggests that the use of information by a company other than that which initially collected it affects consumers' confidence, we have formulated the following hypothesis:

> ***H_2:*** *Internal reuse of information creates a stronger feeling of trust than external reuse.*

Third, the literature states that reuse of information in a context other than that of the initial transaction is the most important factor that influences the feeling of trust regarding respect for privacy on the Internet. This finding regards the pertinence of the reuse. Consequently, the following hypothesis links the pertinence of reuse to the feeling of trust regarding respect for privacy:

> ***H_3:*** *Pertinent reuse of information creates a stronger feeling of trust than does non-pertinent reuse.*

Moreover, marketing strategies that are based on requesting permission from consumers or strategies that use information that consumers have supplied voluntarily tend to increase the feeling of trust regarding respect for privacy. We therefore formulate the following hypothesis:

> ***H_4:*** *Transmission of email creates a feeling of trust that is stronger than that generated by the appearance of a personalized ad.*

As mentioned above, we do not believe that the model that we propose to measure is linear additive. We believe that taken individually, each of the four variables for which we formulate hypotheses might not affect the level of consumers' trust. However, consumers' tolerance threshold may indeed be exceeded by interactions between these same variables that create interactive effects on the feeling of trust. Therefore, even if we do no specify an hypothesis for each and every possible interaction between our variables, we will test for those.

Lastly, in addition to the simple and interactive effects of the four independent variables of the study, two covariables have been included in our conceptual model. We have identified the variables according to the findings concerning attitudes of Internet users in general regarding respect for privacy by Internet sites. The hypotheses we propose relative to these two covariables are stated as follows:

> ***H_5:*** *A more negative attitude toward collection of information will create a weaker feeling of trust in a web site's respect for privacy.*
> ***H_6:*** *A more negative attitude toward reuse of information will create a weaker feeling of trust in a web site's respect for privacy.*

5. METHODOLOGY

Given the nature of the study and the hypotheses to test, an experimental design was adopted as the basic methodology. The experimentation relied on a partial factorial design whereby each of the four variables under study was considered. We thus integrated the experimental conditions in the form of fictitious scenarios that represent a chain of events in a context of navigation on the Internet. All of the participants were subjected to an experimental condition whereby they had to navigate on the Internet and then complete a questionnaire.

In principle, a complete 16-cell factorial plan should have been created, namely: ***2*** (information collection mechanisms: registration form or not) ***X 2*** (marketing strategies put in place: advertisement or email) ***X 2*** (internal reuse, i.e. by the site that gathered the information; or externally, i.e. by another site) ***X 2*** (pertinent or non-pertinent reuse). However, given the structural interactive effect among the information collection mechanisms and the marketing strategy (in cases where there is no registration form, the email strategy could not be applied), 4 of the 16 conditions were removed leading to a partial factorial design. To place the participants in an experimental condition, we constructed 12 experimental Internet sites, which act as guides, detailing the steps that the subjects were required to follow as part of the experiment. The experiment was thus directed by an operator, whose role was to read instructions and notify the participants of the various stages. The operator was in charge of supplying details regarding the collection or reuse of information, depending on the experimental conditions. We chose to conduct the experiment in a laboratory setting and use an operator to ensure that all participants received the same information.

The operator began by providing each of the 120 consumer participants with a verbal description of the study. The description consisted in clarifying to each participant that the study concerned the possible reuse of personal information by Internet sites when users navigate on the site. The operator then provided a general description of the data collection performed by Internet sites, a phase that was identical for all participants. They were told that in general, the Internet sites collect personal information regarding Internet users, either by asking them to complete a form, in which they supplied personal information, or through "cookies." All the participants were then asked to navigate on the Internet site of a DVD vendor and to conduct a search to procure the complete set of Star Wars DVDs. After this phase, more than half of the participants were asked to complete a form to register with this vendor. Following the first phase and after having visited other sites, the consumers were invited to return either to the vendor's site or to the site of a department store, and to pay particular attention to any ads posted or emails received. In all cases we ensured that the participants had adequately read and understood either the ad or the email received. Depending on the case, the operator mentioned that the information reused in the message originated either from the form they had completed or from their navigation, in which case it was gathered by means of a "cookie." The final phase--completing a questionnaire online following the navigation process--was the same for all participants.

5.1 Manipulations

The data collection mechanism was manipulated by asking 80 consumers to complete a questionnaire in which they were required to provide their name, address, phone number, favorite color, favorite pass-time and their email address. The 40 consumers that did not receive a form to complete received a verbal explanation about the fact that a "cookie," would gather information regarding their navigation. To ensure that the two groups realized that information regarding them had indeed been collected and that only the data collection tool varied, one question, intended to test the validity of this manipulation (Perdue and Summers 1986) was inserted in the final questionnaire. This question read as follows: "The (DVD vendor's name) site gathered information concerning me and my navigation." Measured by a 7-point Likert scale, this question confirms that regardless of the data collection method, the two groups realized that information regarding them had been gathered (means: form = 5.98; cookies = 5.70. t = .805; sig. = .424).

The second variable was designed to manipulate the marketing strategy (email or ad). For 8 of the 12 experimental conditions, a banner advertisement appeared during navigation. This advertisement was personalized in 4 of the 8

conditions, namely those where the form comprised the data collection tool. In the 4 other conditions, a general ad was displayed (cookie conditions). For the final 4 conditions, a personalized email was sent.

The third variable, namely reuse of information for advertising purposes, was manipulated either on the site of the initial DVD vendor (manipulation of internal reuse), or on the site of a large department store completely independent from the DVD vendor (external reuse). Six of the twelve experimental conditions featured an advertisement from the initial DVD vendor (internal reuse) whereas the six other conditions proposed an advertisement originating from a large department store (external reuse). To determine the success of this manipulation, we inserted two questions in the final questionnaire. The first "A second site, other than that of (DVD vendor), collected personal information that I supplied," was intended to ensure that consumers exposed to the message from the large department store were more suspicious than consumers that were not exposed to the second retailer that information concerning them had been transmitted to a third party. The second question: "A second site, other than that of (DVD vendor) collected information regarding my navigation," had the same objective, but specifically evaluated consumers' navigation. The two questions included a 7-point Likert scale. A series of two Student's tests demonstrates that the manipulation was well understood and that the consumers that had been approached by the department store felt more strongly than the other consumers that this retailer had gathered personal information (exposed to DVD vendor's message = 4.33; exposed to department store's message = 5.28. t = 1.86, sig. = .039) or information regarding their navigation (4.03 vs 5.40; t = 3.306, sig = .001).

Lastly, the "pertinence of reuse" variable was manipulated according to the content of the message sent to the consumers. Therefore, in both the banner and the email, the message advertised either a special offer on the full set of the Star Wars DVDs in the 6 cases of pertinence of reuse, or a reduction of up to 50% on sofas in the department store in the 6 cases of non-pertinent reuse. Table 1 below illustrates the 12 conditions of our experimental design.

Table 1: Schematic representation of 12 experimental conditions

DIMENSION:	***Data collection mechanism***	**Marketing strategies**	**Reuse (message source) Internal or external**	**Pertinence of reuse**
Manipulation:	*Registration form*	*Ad or email*	DVD vendor or department store site	Content of advertising message/email
	Yes	Advertisement (personalized)	*DVD vendor*	Complete set of Star Wars trilogy
				Sofas in department store
			Department store	Complete set of Star Wars trilogy
				Sofas in department store
		Email	*DVD vendor*	Complete set of Star Wars trilogy
				Sofas in department store
			Department store	Complete set of Star Wars trilogy
				Sofas in department store
	No (cookies)	Advertisement (standard)	*DVD vendor*	Complete set of Star Wars trilogy
				Sofas in department store
			Department store	Complete set of Star Wars trilogy
				Sofas in department store

5.2 Measures

In addition to the four variables manipulated, three variables were measured. The first was intended to measure the propensity to want to provide information to a retailer on the Internet. The second measured the attitude toward reuse of this information by a third party site. For each of these two variables a scale was developed. In both cases the items used were inspired by the work of Kehoe and Pitkow (1996) and Cranor et al. (1999). The first variable is based on a scale that includes 7 items measured on 7 points, whereas the second is based on a 5-item scale measured on 7 points. These two scales emerged following a series of iterations proposed by Churchill (1979). Measurement of the propensity to provide information exhibited high fidelity (alpha = .80) whereas measurement of the attitude toward reuse of private data had an alpha of .82. The discriminant validity of these two measures was very high in both cases; following a principal component analysis each measure emerged as a unique factor (eigenvalues of = 1.6 and 5.1 respectively).

The third variable of this study was intended to measure the degree of consumers' trust in the DVD vendor's site, that is the site at which information was gathered. This variable, which constitutes the dependent variable of our experiment, was measured by a two-item scale, namely "I sufficiently trust the (vendor's name) site on which I just surfed to supply personalized information again," and "I trust in the security of the commercial transactions on the site on which I am navigating." These items, taken from Kehoe and Pitkow (1996) display a Cronbach's alpha of .88.

The study was conducted on 120 consumers in a laboratory setting. The subjects were all familiar with Internet use and had all navigated on a commercial site at least once. Consumers were recruited by a hyperlink placed on the site of a large construction product retailer situated in northeastern North America. Three quarters of the participants had been using the Internet for over 3 years. In addition, 44% of the subjects had been using the Internet for between 1 and 3 hours per day for navigation, compared with only 14% that used it for less than half an hour per day. Regarding purchasing on the Internet, 56% of the consumers had already made a purchase on the Internet. Moreover, only 28% had made a purchase on the Internet in the past month. Lastly, 66% of the participants reported that they purchased a good or service directly from a physical retailer, i.e. not via the Internet, but based on information gathered on the Internet. General demographics, age, sex and revenue, were in line with the population.

Since the level of experience that a consumer has with the internet could influence his attitude toward privacy on the net we conducted two test to determine whether the level of experience and the usage rate of the Internet could have an impact on the predisposition of consumers to provide information or on their attitude toward the reuse of information. Neither the attitude toward gathering of information nor the attitude toward reuse of information seem to be influenced by the frequency with which consumers navigate the Internet, nor by the number of years of experience using the Internet.

6. ANALYSES AND RESULTS

To test the study hypotheses, and given that the study is based on a factoral experimentation design, a covariance analysis (ANCOVA) was performed. The results are presented in Table 2 below. As two of the variables manipulated were systematically linked (the method used to gather information and the strategy used to disseminate the message) the experimental design was not a full design. Consequently, only certain double or triple interactions and no quadruple interaction of the variables could be tested. Nonetheless, the results clearly demonstrate the interactive effects of the variables studied.

Table 2 : Covariance Analysis (ANCOVA)

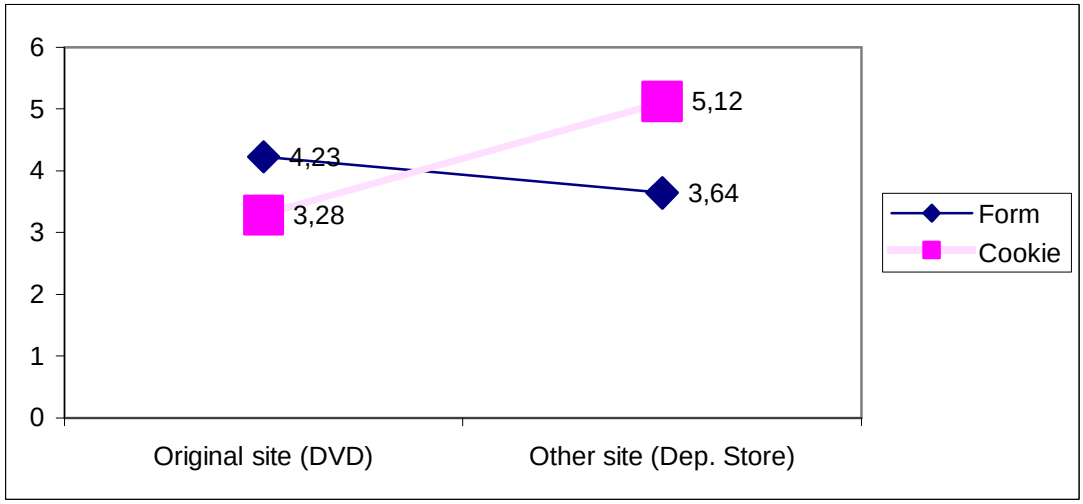
Dependant variable: Confidence in the site with regard to privacy

Source of variation	Sum of square roots	Degrees of freedom	F	Sig.
Predisposition to provide information	**33.065**	**1**	**9.856**	**.002**
Attitude toward reuse of information	4.671	13	1.392	.241
Collection method	.943	1	.281	.597
Marketing strategy	.277	1	.082	.775
Internal or external reuse	.373	1	.111	.740
Pertinence of reuse	9.221E-02	1	.027	.896
Method x Site	**11.130**	**1**	**3.318**	**.072**
Mechanism x Strategy	*.000*	*0*		
Method x Pertinence	1.102	1	.328	.568
Strategy x Site	**20.983**	**1**	**6.255**	**.014**
Strategy x Pertinence	2.351	1	.701	.405
Site x Pertinence	.292	1	.087	.769
Method x Site x Strategy	*.000*	*0*		
Method x Site x Pertinence	.773	1	.231	.632
Method x Strategy x Pertinence	*.000*	*0*		
Strategy x Site x Pertinence	3.835^{E}-02	1	.011	.915
Method x Site x Strategy x Pertinence	*.000*	*0*		

As Table 2 reveals, no simple effect is significant. Thus taken independently, the four variables studied do not have an impact on consumers' feeling of trust in a company to which they have provided personal information. Although non-significant and thus leading to rejection of hypotheses 1, 2, 3 and 4, these results are still noteworthy. In effect, the results clearly demonstrate that in general, consumers are tolerant toward various manifestations of relationship marketing that may occur on the web. Therefore, the collection of personal information by either a form or a cookie does not seem to affect their consumers' trust in the company that gathers the information. In addition, whether these consumers are later contacted by the same company or by another company, via an advertisement or an email, and regardless of whether this advertisement is pertinent or not, their trust generally does not seem to be significantly affected.

If consumers' confidence does not appear to be affected by any of the four variables investigated in this study, examination of the combined impact of the same variables reveals a substantially different reaction. Accordingly, as shown in Table 2 and Graph 1 below, there is an interactive effect between the way in which personal information is collected (form or cookie) and the reuse of this information by the original site visited or another site.

Figure 1: Average feeling of trust of Internet users in a site's respect for privacy according to which site reuses the information and the data collection method



Therefore, the impact on the feeling of trust regarding respect for privacy, measured on a 7-point sacle, is affected when another site enters the picture, depending on the way in which the information is initially collected. When consumers receive an advertisement from a site other than the initial site without the second site's having solicited the information by means of a questionnaire, their feeling of trust does not decrease, but rather increases. In contrast, when the initial information source is a form and consumers are subsequently contacted by a third party site, their level of trust in the initial site decreases sharply. This decrease results from the fact that the message is personalized. When personalization is performed by the initial site, consumer confidence increases (3.28 vs. 4.23). Yet when the message originates from another site, it is markedly preferable, in terms of trust in the second site, that it is not personalized (5.12 vs 3.64). This can be explained by the fact that Internet users are basically convinced that the quantity of information available regarding them on the Internet is smaller if they have not supplied it directly (Caudill and Murphy, 2000; Cranor et al., 1999; Miyazaki and Fernandez, 2001).

Furthermore, a second interactive effect significantly impacts Internet users' feeling of trust, namely that between the site that reuses the information and the marketing strategy put in place. As Graph 2 illustrates, the feeling of trust regarding respect for privacy is particularly affected when another site uses email as a communication strategy. Accordingly, the feeling of trust in the site drastically decreases when another site sends an email. In addition, we observed that the use of an advertising banner strategy by a second site does not negatively affect trust in the initial site that gathered the information. Therefore, maintaining relations with the clientele through email rather than simple advertisements increases consumers' trust in the original site, whereas the inverse reaction is triggered by identical communication from a third party.

Figure 2: Average feeling of trust of Internet users in a site's respect for privacy depending on whether the site reuses information and the marketing strategy

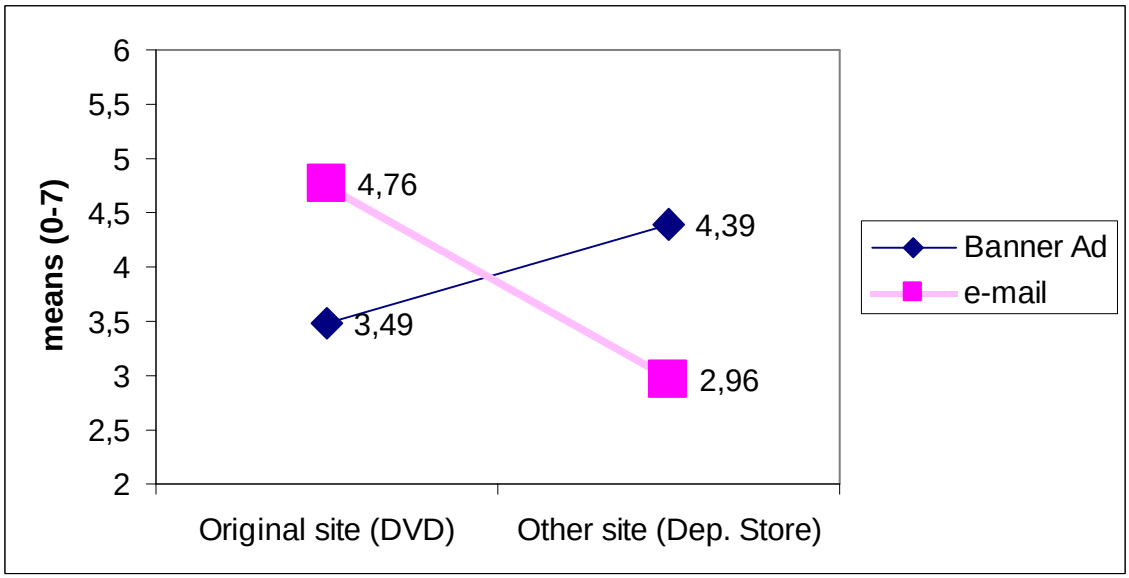


Table 2 illustrates the mediating role of consumers' predisposition to provide information in the feeling of trust in the initial site (F = 9.856, sig. = 0.002; r = .278; sign = .002). Specifically, the less consumers are predisposed to provide information, the less trust they have in the site in which they have provided such information. These results confirm hypothesis H5. Moreover, although it is in the expected direction, hypothesis H6, which links the consumers' attitudes toward reuse of information to the feeling of trust placed in the initial site, could not be affirmed (F = 1.392, sig. = .241; r = .120; sig. = .190).

6. CONCLUSIONS AND IMPLICATIONS

The results of our study demonstrate that when an Internet site reuses information initially gathered by another site, consumers' trust in the original site is compromised. This observation corroborates Novak et al. (1998), who documents Internet users' inherent fear that sites that gather information will subsequently sell it to another site. The results of our variance analysis reveal that the marketing strategy whereby a second site sends email greatly decreases Internet users' trust in the data gathering site's respect for their privacy. Note that whereas this marketing strategy, often called permission marketing, is currently expanding vigorously, we have found that this form of marketing is effective only if the message is expected, personalized and pertinent (Godin, 1999). In the case of an email sent by a site other than the original site, as was the case in our experiment, it is not surprising to observe that this strategy diminishes Internet users' trust in the initial site.

Concerning the pertinence of reuse of information, our analyses have not enabled us to conclude that there is a significant effect on Internet users' feeling of trust in a site's respect for their privacy. Nonetheless, several researchers have suggested that the factor concerning reuse of information that most strongly influences consumers' feeling of trust in a company's respect for their privacy is the reuse of information in any context other than that of the original collection (Cranor et al., 1999; Culnan, 1995). The lack of conclusiveness of our results on this dimension may be attributable to our manipulation of pertinence not being sufficiently strong.

In conclusion, the study results therefore partially validate our hypotheses. First, they clearly demonstrate that Internet users' feeling of trust in Internet sites' respect for their privacy is notably influenced by the act of collecting information and by the interaction of certain elements related to the reuse of this information. These elements create points of sensitivity that cause initially tolerant Internet users to become more suspicious of sites to which they supplied information. Accordingly, we observed that Internet users are aware of multiple realities related to collection and reuse of their personal information by Internet sites.

Marketing managers can draw two noteworthy conclusions from these results. First, consumers are generally tolerant of certain marketing practices. In contrast, and this is the most important finding, they may turn against a company in which they have placed their trust if they feel betrayed. This phenomenon is particularly evident when consumers realize that the information they provided voluntarily in a form has been transmitted to a third party company. Even worse, their trust is particularly jeopardized when third party companies contact consumers through personalized emails. In short, if the permission marketing practice is growing steadily, and while it may often represent an opportunity for a company to generate revenues by reselling its customer list, it also poses risks to that company.

References

Ang, L., C. Dubelaar et B.-C. Lee (2001), « To Trust or Not to Trust? A Model of Internet Trust from the Customer's Point of View », *14th Bled Electronic Commerce Conference*,Bled, Slovenia (June) 2001, http://www.uow.edu.au/~boon/Bled2001.pdf

Burgoon, Judee K. (1982), « Privacy and Communication », *Communication Yearbook 6*, (Michael Burgoon, ed.) Beverly Hills : Sage.

Caudill, E. M. et P. E. Murphy (2000), « Consumer Online Privacy: Legal and Ethical Issues », *Journal of Public Policy and Marketing*, Vol. 19, No 1, (Spring) pp. 7-19.

Charters, D. (2002), « Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience », *Journal of Business Ethics*, Vol. 35, pp. 243-254.

Churchill, G. A. (1979), « A Paradigm for Developing Better Measures of Marketing Constructs », *Journal of Marketing Research*, Vol. 16, No 1, February, pp. 64-73.

Cranor, L. F., J. Reagle et M. S. Ackerman (1999), « Beyond Concern: Understanding Net Users' Attitudes About Online Privacy », AT&T Labs-Research Technical Report TR 99.4.3, 14 . April (http://research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm

Culnan, M. J. (1993), « How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use », *MIS Quarterly*, Vol. 17, No 3, September, pp. 341-363.

_____ (1995), « Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing », *Journal of Direct Marketing*, Vol. 9, No 2, Spring, pp. 10-19.

_____ (2000), « Protecting Privacy Online : Is Self-Regulation Working », *Journal of Public Policy and Marketing*, Vol. 19, No 1, Spring, pp. 20-26.

_____ et P. K. Armstrong (1999), « Information Privacy Procedural Fairness, and Impersonal Trust: An Empirical Investigation », *Organization Science*, Vol. 10, No 1, janvier-février, pp. 104-115.

_____ et S. J. Milberg (1999), « Consumer Privacy », in Information Privacy: Looking Forward, Looking Back, (Mary J. Culnan, Robert J. Bries and Michael B. Levy, eds.) Georgetown University Press.

Federal Trade Commission (FTC) (1998), « Privacy Online: A Report to Congress », June 1998, (http://www.ftc.gov/reports/privacy3/priv-23a.pdf)

_____(2000), « Privacy Online: Fair Information Practices in the Electronic Marketplace », A Report to Congress, May 2000, (http://www.ftc.gov/reports/ privacy2000/privacy2000.pdf)

Glickman, J. A. (2000), « Personalizing the Internet: The new one-to-one marketing », *Direct Marketing*, Vol. 63, No 1, May, pp. 54-57.

Godin, S. (1999), Permission marketing: turning strangers into friends, and friends into customers (New York: Simon & Schuster), 155 p.

Goodwin, C. (1991), « Privacy : Recognition of a Consumer Right », *Journal of Public Policy and Marketing*, Vol. 10, No 1, (Spring), pp. 149-66.

Han, P. et A. Maclaurin (2002), « Do consumers really care about online privacy? », *Marketing Management*, Vol. 11, No 1,(January), pp. 35-38.

Kehoe , Colleen M. and Jim Pitkow, (1996) « Surveying the Territory: GVU's Five WWW User Surveys» *The World Wide Web Journal*, Vol. 1, no. 3, 1996, p. 77-84

Lombard, M. et J. Snyder-Duch (2001), « Interactive Advertising and Presence: A Framework », *Journal of Interactive Advertising*, Vol. 1, No 2,(Spring)

Louis Harris & Associates (1999), « IBM Multi-National Consumer Privacy Survey », (http://www-3.ibm.com/security/library/wp_priv-survey.shtml)

Milne, G. R. (1997), « Consumer Participation in Mailing Lists : A Field Experiment », *Journal of Public Policy and Marketing*, Vol. 16, No 3, (Fall), pp. 298-309.

_____(2000), « Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue », *Journal of Public Policy and Marketing*, Vol. 19, No 1, (Spring), pp. 1-6.

_____ et M.-E. Boza (1998), « A Business Perspective on Database Marketing and Consumer Privacy Practices », *Marketing Science Institute Working Paper No 98-110*, Cambridge, MA : Marketing Science Institute.

_____, M.-E. Boza et A. J. Rohm (1999), « Controlling Personal Information in Marketing Databases: A Consumer Perspective », in *1999 Winter AMA Proceedings*.

_____ et A. J. Rohm (2000), « Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives », *Journal of Public Policy and Marketing*, Vol. 19, No 2, (Fall) , pp. 238-249.

Miyazaki, A. D. et A. Fernandez (2000), « Internet Privacy and Security: An Examination of Online Retailer Disclosures », *Journal of Public Policy & Marketing*, Vol. 19, No 1, (Spring) pp. 54-61.

_____ et _____ (2001), « Consumer Perceptions of Privacy and Security Risks for Online Shopping », *Journal of Consumer Affairs*, Vol. 35, No 1, pp. 27-44.

Novak, T. P., D. L. Hoffman et M. A. Peralta (1997), « Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web », in « Anonymous Communications on the Internet: Uses and Abuses », http://www2000.ogsm.vanderbilt.edu/papers/anonymity/anonymity2_nov10.htm]

_____, _____ et _____ (1998), « Building Consumer Trust in Online Environments: The Case for Information Privacy », http://www2000.ogsm.vanderbilt.edu/papers/CACM.privacy99/CACM.privacy99.htm)

Nowak, G. J. et J. Phelps (automne 1992), « Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs », *Journal of Direct Marketing*, Vol. 6, No 4, pp. 28-39.

Peppers, D. et M. Rogers (1993), « Viewer Privacy in the Interactive Age », *New York Times*, août 1993, F11.

Prabhaker, Paul R. (2000), « Who Owns the Online Consumer? », *Journal of Consumer Marketing*, Vol. 17, No 2.

Rohm, A. J. et G. R. Milne (1998), « Emerging Marketing and Policy Issues in Electronic Commerce: Attitudes and Beliefs of Internet Users », in *1998 Marketing and Public Policy Conference Proceedings*, (Vol. 8), (Alan Andreason, Alex Simonson et N. Craig Smith, eds.) , American Marketing Association, pp. 73-79.

Sheehan, K. B. et M. Grubbs Hoy (1999), « Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns », *Journal of Advertising*, Vol. 28, No 3, automne, pp. 37-51.

_____ et _____ (2000), « Dimensions of Privacy Concern Among Online Consumers », *Journal of Public Policy and Marketing*, Vol. 19, No 1, (Spring), pp. 62-73.

Smith, R. E. (1980), *Privacy: How to Protect what's Left of It* (New York, Anchor Books), p. 313-315.

Wang, H., M. K. O. Lee et C. Wang (1998), « Consumer Privacy Concerns About Internet Marketing », *Association for Computing Machinery, Communications of the ACM*, Vol. 41, No 3, mai, pp. 63-70.

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