WEB MERCHANTS' PRIVACY AND SECURITY STATEMENTS: HOW REASSURING ARE THEY FOR CONSUMERS? A TWO-SIDED APPROACH

Claire Gauzente
LARGO - University of Angers, France
claire.gauzente@univ-angers.fr

ABSTRACT

Online environment is now part of everyday life. However, trust is still an important issue for online merchants. This explains why there is an increasing interest in "trust busters" by the general consumer. Trust busters entail, among other, a thorough online privacy policy (OPP) that encompasses detailed privacy and security statements. The paper looks at both the views of the consumer and the views of the web merchants in attempting to unravel the problems of privacy on the Net. A sample of 89 French web merchants and a sample of 154 consumers were examined using bivariate analysis.

The results show that, even in a government-regulated country such as France, there is still room for improvement in web merchants' privacy policies. Concerning consumers, an important result is that the perception of reassuring privacy and security statements varies according to browsing intention.

Keywords: privacy statements, security statements, sites' practices, consumers' perceptions, reassurance.

1. Introduction

The issue of privacy in commerce is far from being a new one (Nowak and Phelps, 1992; Mason, 1995). Indeed, the development of database marketing and direct marketing has already opened up the privacy debate some time ago. In the last decade, the number of articles in the area has increased considerably (Roznowski, 2003). However with the WWW revolution, it has become all the more sensitive with important implications for the online marketspace (Hoffman, Novak and Peralta, 1999 a and b; Caudill and Murphy, 2000; Kelly and Rowland, 2000; Nugent and Raisinghani, 2002). As incredible opportunities to collect, store and use information about consumers arise, the question of obtaining data in an ethical manner is getting more important.

Ethical online marketing (Gauzente and Ranchhod, 2001) will definitely become the key to e-competitiveness (Shin, 2001). In order to cope with it, Godin (1999), Barwise and Strong (2002) propose and explore the concept of permission-based marketing. The suggested idea is that when consumers agree to provide information and receive commercial solicitations, marketing can become more personalized and more efficient. Although highly seductive, this principle is moderated by practical limitations. Barwise and Strong (op. cit.) reveal that permission-based advertising should be perfectly targeted, humorous, short, and… not too personal. Tezinde, Smith and Murphy (2002) also underline that, although permission can be given, it does not necessarily correspond to a sincere one (wrong or unused emails are given); and, after a while, received ads can be judged as spam/UCE (Unsolicited Commercial Email). Asking for permission alone does not absolve the marketer from privacy and ethical marketing practice.

Engaging in reflection about privacy requires that a statement of practice is created and that consumers' perceptions are properly understood.

For web merchants, initiatives such as the ones produced by the Federal Trade Commission (Culnan, 1999 a and b) help firms to benchmark their position. The US is a country where the issue of privacy is left to self-regulation (Gillin, 2000) whereas in Europe privacy regulation is government-based, which can be seen from the 8th Article of the European Convention on Human Rights (1963) and the new Directive on Privacy and Electronic Communication (2003). As underlined by Ang (2001), privacy is explicitly classified as a fundamental right in European countries while it is open to more ambiguity in US (privacy is considered to be implied).

From the consumer standpoint, most of the studies focus on user's privacy concerns on the Internet but neglect consumer view on features that are reassuring and ones that are not. In this paper, we advocate that a two-sided stance should be taken, as perceived privacy and perceived security result from interaction between web merchants and their consumers.

This study explores French web merchants' online privacy and security statements and tests a set of hypotheses concerning the perception of privacy and security statements. To our best knowledge, this represents the first

attempt to bring together sites data and consumer data. From a theoretical point of view, the study will contribute to a better understanding of privacy and security concern, as the delineation of these two notions is multidimensional and fluctuating according to philosophical, sociological, legal and individual considerations. From an empirical standpoint, it will add to our knowledge concerning when and why consumers feel concerned about privacy matters and which personal information is deemed as being private (as all 'personal' information may not always be 'private'). Lastly, from a managerial point of view, this study will help web merchants to grasp whether they can build trust from their privacy and security statements the priority areas that should be addressed.

2. Literature Review

2.1. Theories of privacy

The definition of privacy is particularly delicate, as there is no general agreement. Philosophical, sociological, legal and individual aspects are intertwined which leaves room for varying conceptualizations. Before focusing on privacy in the online environment, it is worth taking a look at the different views of privacy (Kelly and Rowland, op. cit.).

Privacy is a constant issue for lawyers and philosophers (Johnson, 1992). In his comprehensive study of privacy conceptualizations, Solove (2003), building partly on Johnson (op. cit.), underlines that six conceptualizations of privacy can be ascertained, with some overlap between them.

One of the most common views of privacy is *the right to be let alon*e, this idea can be traced to the Warren and Brandeis article written in 1890 (quoted in Solove, op. cit.). A variant, more sophisticated, view is privacy as *limited access to the self*. Contrary to the first view, privacy is not equivalent to solitude. Contemporary privacy theorists subscribe to this view where "the right to privacy entitles one to exclude others from watching, utilizing, invading his private realm" (Van den Haag quoted in Solove, op. cit.). This underlines that privacy is a matter of one's relationship to others and the society.

Another view considers that privacy is *secrecy*. Here, privacy is violated by public disclosure of concealed information. In this view, protecting privacy means that information disclosure is avoided. The view that privacy is *control over personal information* tends to be quite predominant. However, as stated by Solove (op. cit.), personal information is not necessarily private information. Moreover, he suggests that limiting privacy to information aspects is too narrow. Another approach considers privacy as *a form of personhood protection*. This concept suggests that privacy is a condition where a person is allowed to keep her individuality, dignity and autonomy. However, it neglects the fact that privacy cannot be limited to the self or the person. The concept of privacy might also span family and friends, hence enlarging the private realm. The scope of this private sphere does not only depend on individual characteristics but also on factors such as culture and historical periods. In some cultures privacy is highly respected whereas in cultures that are more open, some aspects of privacy may not be so important. Also certain historic periods valued privacy whereas others have invaded privacy (privacy of Catholic worship in Protestant England was often invaded).

The last view understands privacy as a form of *intimacy*. This view goes beyond an individualistic definition of privacy and integrates human relationships.

2.2. Conceptualizing online privacy

Clearly, as the above discussion indicates, there is no perfect definition of privacy. This then makes the definition of online privacy even more difficult to create. In research domains such as marketing, management, information systems, the terminology about privacy keeps fluctuating. Academic literature uses terms such as consumer online privacy, information privacy, Internet privacy, privacy concern, and perceived privacy. Belanger et al. (2002) observe that the conceptualizations are also varied. Some studies entail security as one of the dimensions of privacy. Others consider the two notions to be separate concepts. The different studies by Culnan (1999 a and b) as well as the Federal Trade Commission reports suggest that security can be understood as a part of privacy policies. In these contributions, online privacy policy is understood as the set of statements explaining how consumer privacy is dealt with and protected (or secured) by the web merchant. Nevertheless, it is clear that security pertaining to online privacy is not the sole aspect of online security.

Hoffman, Novak and Schlosser (2000) consider that privacy entails environmental control, which determines the security of online shopping and secondary use of information, control. Pavlou and Chellappa (2001) distinguish the two concepts as well as Belanger et al. (op. cit.). The following table summarizes different views of privacy used in studies (see table 1.).

Table 1: A selection of privacy definitions in relation with Internet environment

Terminology / Definition	Authors
Privacy protection for the Internet / …is widely understood as the right of individuals to control the collection, use and dissemination of their personal information that is held by others.	EPIC – Electronic Privacy Information Center
Information privacy / The ability of an individual to control the access that others have to personal information	Hoffman, Novak and Peralta (1999 a and b)
Consumer privacy / …a subset of privacy described as a two-dimensional construct involving physical space and information.	Caudill and Murphy (2000)
Informational privacy / in electronic commerce …/… the right of individuals to exercise control over information about themselves.	Kelly and Rowland (2000)
Perceived privacy / The subjective probability with which consumers believe that the collection and subsequent access, use and disclosure of their private and personal information is consistent with their confident expectations.	Pavlou and Chellappa (2001)
Privacy / …is the ability to manage information about oneself.	Belanger, Hiller and Smith (2002)

From these definitions, it appears that consumer privacy in the Internet environment is both individual-centered and information-focused. Compared to previously described privacy theories (Solove, op. cit., Johnson, op. cit.) this is a narrower view of privacy. For the present study, this narrower view is however relevant. As for the security aspects, we will follow the Culnan (op. cit.) and FTC (op. cit.) orientations where online privacy entails certain aspects of security, especially those regarding the protection of consumers' information.

2.3. Review of studies on online privacy and security

The privacy and security issue entails two complementary sides. The first corresponds to what web merchants' claim about privacy and security. These can be presented in various forms (mere sentences, paragraph or developed policy designated as OPP – Online Privacy Policy). The second side corresponds to consumers' perceptions.

Websites online privacy policies. Concerning web merchants' OPP, few empirical studies can be found. Culnan's reports (1999 a and b) were the first ones. Two samples were used. The first sample consisted of most frequently visited web sites and the second of 100 top commercial web sites. The results showed that a majority (65.9%) of web sites integrates privacy/security statements, but this ranges from a discrete statement to a comprehensive chart. A French duplication of Culnan' surveys in 2002 (Gauzente, 2003) exhibits that French sites tend to use complete OPP rather than discrete statements (80%). A US-UK-France comparison of web merchants' OPP and personalization features shows that the two European countries rely on a more formal model of OPP than the US (Gurau, Ranchhod and Gauzente, 2003).

Palmer, Bailey and Faraj (2000) give complementary insights in their study. The mix of OPP and Trusted Third Parties is examined (TTP are the set of organizations that try to promote trust on the Web such as the French L@belsite or the American TRUSTe). Certain web sites might want to simply use TTP instead of an OPP. Their study shows that the mix of the two depends on the web site's insertion in the web and its notoriety. In particular, as notoriety and web insertion increase, OPP and TPP appear less necessary and are less prominent in the site's architecture.

The consumer's view. The privacy issue is more researched from a consumer's perspective (Teltzrow and Kobsa, 2003). Hoffman, Novak and Peralta (1999a) use 1997 panel data to study consumers' privacy concern. It appears that consumers are highly concerned with privacy in web environment (above 60% of US consumers), which is not the case for other traditional media because consumers' need for control and protection is increased in Internet environment. Consumers are also conscious that data are important for marketers in order to tailor products and services, therefore illustrating the paradox of privacy vs. personalization (Mabley, 2000; Evans, 2003). According to these authors, a key explanation of privacy concern is the concept of control (Hoffman, Novak and Peralta, 1999b), which entails environment control (the perception of security) and the secondary use of information control. A view offered by Culnan and Armstrong (1999) insists that privacy should not be an issue provided that web sites

implement a fair policy. This underlines the importance of perceptions. The Culnan and Milne report (2001) indicates that 82% of consumers have already refused to give personal information because it was deemed too personal or unnecessary. In this study, a proportion of 81% of consumers indicates that they want to protect themselves against privacy risks. However, 50% of consumers also acknowledge that they do not read web privacy notice from web sites. Two main reasons for this: (1) consumers trust well-known companies but also (2) privacy notices are deemed uneasy to understand. Indeed, Han and Maclaurin (2002) insist on the explicitness of privacy policy to clear consumers' fears.

The importance of perceived privacy[1]. According to the literature, consumer's perception of privacy is central for online commerce for at least three reasons. The main reason is that perceived privacy is hypothesized to contribute to the formation of trust. Hence, most of the privacy studies integrate this central relationship. A second, clearly related, one is that privacy perception is linked to risk assessment. The third consequence of perceived privacy is its impact on purchase intention and behavior.

With the exception of Culnan's studies on privacy, Pavlou and Chellappa (2001) conducted one of the first empirical studies that links perceived privacy and trust. This study focuses on perceived privacy and perceived security of web sites and their contribution to trust. The results indicate that although perceived privacy is a significant contributor to trust, perceived security is more important. Yoon's study (2002) confirms that transaction security is significantly linked with trust.

Researches conducted by Sultan et al. (2003) and Shankar, Urban and Sultan (2002) are focused on the formation of online trust. The large scale study by Sultan et al. (op. cit.) uses a sample of 6831 consumers and reveals that although privacy and security are significantly linked to trust, 80% of the explained variance of trust is due to other variables such as navigation, brand, advice.

Belanger et al. (2002) have conceptualized privacy, along with security features, third party privacy seals and third party security seals, as trust indices. As consumers need reassurance because they perceive online purchasing as an uncertain and risky situation, privacy statements are considered as contributors to trust. Building on previous researches, the authors hypothesize that security features will be more important than privacy features in the eyes of consumers, which is confirmed by empirical results.

From these studies, privacy appears to be a real contributor to online trust but is not as powerful as security. Several explanations can be proposed. One is that privacy is becoming a less sensitive matter over as time, as consumers get used to the Internet (Sultan et al., op. cit.) and to the techniques that can be used to protect their privacy. This can be linked to Luo's suggestion (2002) that institutional mechanisms (such as third parties, banks, and government regulators) have the potential to reduce the concerns about privacy and to increase trust. The current development of institutional mechanisms might explain that although privacy remains an issue for consumers, it is no longer an obstacle to trust formation.

Belanger et al. (op. cit.) argue that it is possible that consumers understand better the notion of security than the one of privacy.

Additionally, building upon the review of Grabner-Kräuter and Kaluscha (2003), it is also possible that considering two aspects of trust should help to refine the link between perceived privacy and trust. Briefly, trust can be conceptualized either as the belief that the other party will be honest (trusting belief) or it can be understood as the intention to depend on the other party (trusting intention). It is possible that perceived privacy has a stronger link with trusting beliefs than with trusting intentions.

Lastly, the relationship is probably a reciprocal one. Luo (op. cit.) proposes that trust can lower privacy concern, which does not necessarily ease the study of perceived privacy and trust.

A second, closely linked, reason why privacy is deemed so important in electronic commerce is that it contributes to consumers' risk perception. Miyazaki and Fernandez (2001) suggest that privacy and security are dimensions of risk for online shopping. However, results indicate that even if consumers perceive privacy risks it does not necessarily affect their purchase intention. In his study of consumer's perceived risk in online purchase, Lim (2003) regards privacy as a source of perceived risk. This type of risk is related to technology (is the technology reliable from a privacy standpoint?) and to the e-vendor. The results, based on focus groups, indicate that consumers consider Internet security to be important, even when 'lock' symbols appears on web sites. Concerning the e-vendor's characteristics, consumers are very cautious about web merchants that ask for unnecessary questions during transaction and about those who do not provide privacy policy.

Lastly, perceived privacy is also thought to contribute directly to online purchase. While some of the previous studies suggest that privacy concern does not necessarily affect purchase intention (Mizayaki and Fernandez, op.

[1] We use the term privacy but security features can be included in some of the reviewed studies.

cit.; Belanger et al., op. cit.) some others suggest that it might remain an issue. Although not focused on online transactions, the study of Phelps, D'Souza and Nowak (2001) helps in understanding the behavioral consequences of privacy concerns. Their results show that as privacy concern increases, weaker purchase experience (in terms of recency, frequency and amount) is observed among consumers. The Culnan and Milne report (op. cit.) corroborates such findings: 64% of consumers decided not to use a web site or to buy something from a web site because they were not sure how their personal information would be used. In sum, it remains uncertain whether perceived privacy is directly linked to purchase intention and behavior.

Hypotheses about the antecedents and consequences of privacy concern. Privacy concern cannot be considered as an intangible state, it is subject to variations according to the individual, to the state of technology and to the web merchant's characteristics, in particular their online privacy and security statements. Taking this into account, we suggest that both consumers and web merchants should be examined. A first step is thus to answer the following question:

Q: What is the current state of web merchants' privacy and security statements?

A second step is then to understand the role of privacy concern and to assess to which degree web merchants' privacy and security statements can reduce privacy concern by reassuring consumers.

Milberg et al. (1995) studied privacy concerns as they relate to nationality, regulatory systems and gender. Their results show that females tend to be more concerned than males. This appears to be confirmed in the study by Sheehan (1999). However, Dommeyer and Gross (2003) obtained non-significant results on a related topic: privacy protection awareness and use of protection laws exhibit no difference between males and females. They also investigated the effect of age on privacy protection use and privacy awareness, finding that the expected positive relationship between the two was contradicted by empirical results with younger people tending to use a protection strategy more often than their elders. This probably indicates a greater degree of awareness amongst younger users of the potential problems on the Internet. The older generation is also concerned about security and protection, but is less aware of the operational issues.

Most authors report that web usage and consumer's web experience is a key variable for online trust and risk perception (Jarvenpaa, Tractinsky and Saarinen, 1999, Mizayaki and Fernandez, op. cit., Shankar, Urban and Sultan, op. cit., Lim, op. cit., Corbitt, Thanasankit and Yi, 2003, Grabner-Krauter and Kaluscha, op. cit.). A logical proposition is that it also affects privacy concerns. Experienced, frequent users will be probably less pre-occupied with privacy matters. Hence, it is proposed that:

H1: Consumer characteristics impact on privacy concerns.

In particular, females are expected to feel more concerned about privacy than males (*H1a*). Younger people are expected to be less concerned about privacy than their elders (*H1b*).

Expert web users will feel less concerned about privacy than beginners (*H1c*). Frequent web users will feel less concerned about privacy than occasional ones (*H1d*). Users who benefit from high speed Internet connection will feel less concerned about privacy than those who have low Internet connection (*H1e*).

Previous research on perceived privacy and purchase intention (Culnan and Armstrong, op. cit., Han and Mclaurin, op. cit., Phelps, D'Souza and Nowak, op. cit.) indicate that privacy concern is lessened as the consumer's intention to purchase increases. Thus, privacy concern is likely to depend on the moment and type of browsing. When consumers simply browse (for instance, for fun, or just strolling), they will probably feel more concerned about privacy than when they require information from the web merchants or even when they intend to purchase from the site. The following hypothesis is proposed:

H2: Consumers' intentions when browsing on the Internet impacts privacy concern.

Web users browsing for buying purpose will be less concerned than those requiring information and those who are simply browsing at will.

Schoenbachler and Gordon (2002) indicate that when trust is established, consumers tend to provide personal information on a more voluntary basis. If we follow the logic according to which privacy concern impacts trust building and willingness to provide information, it can be suggested that when privacy concern is high, the reluctance to provide information will be high, too. This leads to the following hypothesis:

H3: When privacy concern is high, the consumer will be highly reluctant to provide personal information.

The Belanger et al. (op. cit.) study indicates that, privacy and security statements are linked to trustworthiness of web sites. An understanding of why these trust indices become important is also of interest. A logical explanation of the importance granted to these indices is that consumers feel highly concerned about privacy and security. Hence, it is proposed that:

H4: The higher the privacy concern is, the more reassuring web merchants' privacy and security statements will be perceived.

Belanger et al. (op. cit.) also identify the relative importance of trust indices (that is: privacy statements,

security features, third party privacy seals, third party security seals) in the eyes of consumers. Their results show that security features are more important than other trust indices. This is coherent with other studies (Pavlou and Chellappa, op. cit., Mizayaki and Fernandez, op. cit.). However, concerning detailed privacy and security statements, it remains unclear as to what types of statements are the most reassuring for consumers. Hence, it is suggested that there exists a hierarchy between privacy and security statements and that within privacy statements those pertaining to the control of one's information are particularly important (Hoffman, Novak and Schlosser, op. cit.).

H5: There exists a hierarchy of trust between privacy and security statements.
Security statements are expected to be perceived as more reassuring than privacy statements. Additionally, privacy statements pertaining to information control are expected to be perceived as more reassuring than other privacy statements.

The following research model can be drawn. As suggested previously, the matter of consumers' privacy cannot be studied without a sense of what web merchants' state concerning privacy and security. Web merchants' practices in this domain impacts consumer's perception, this gives rise to our research question (Q). The study of consumer's privacy concern and its impacts on the perception of reassuring privacy and security statements is then proposed (H1 through H5).

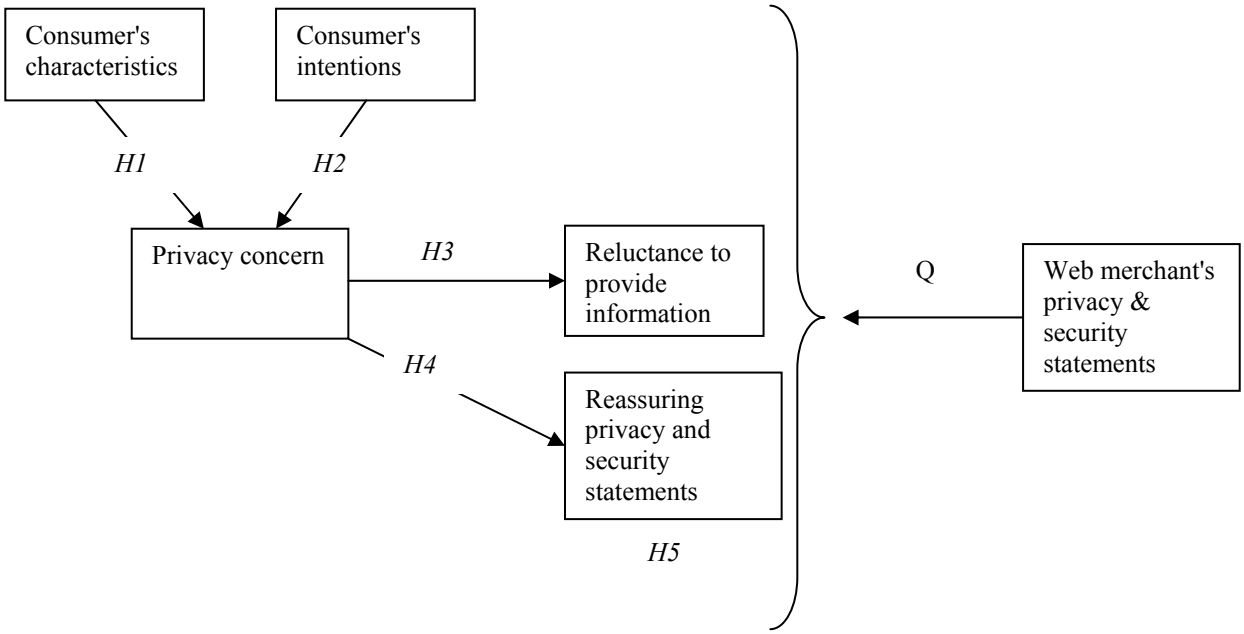

Figure 1: Research Model

3. Method

3.1. Web merchants survey

Survey instrument. The visit guide is an adapted version of Culnan's guide used for the Federal Trade Commission Survey (1999). Culnan's original instrument entails five aspects of online privacy policy: notice, choice, access, security, and contact. This helps to give a general picture of the web site's policy but it needs to be refined for web merchants. In particular, we have distinguished two types of data: personal and financial as the financial matter is often a sensitive one (Culnan and Milne, op. cit., Schoenbachler and Gordon, op. cit.). Following Gauzente and Ranchhod (2001), we also included horizon as a complementary criterion in order to assess privacy and security statements. This criterion corresponds to the time-length during which personal data are stored and used. An ethical practice would be to indicate to consumers how long their data will be stored and used and would even be to give them the choice of the time-period during which their data can be exploited. Overall, we will consider that a thorough online privacy policy includes privacy and security statements on at least 5 the following 6 aspects: notice, choice, access, security, horizon, and contact.

Specific to France, is the CNIL mention. The Commission Nationale Informatique et Libertés was established by the Information Privacy Law in 1978 (www.cnil.fr) and is empowered to issue recommendations and legally

binding opinions on issues concerning privacy. It also controls to what extent firms respect law. Any firm has to register and obtain a CNIL number. For web merchants, this should be indicated on their sites. This information will also be collected in order to assess whether web merchants go beyond mere legal CNIL statements.

The visit guide also includes descriptive features such as web merchants sector of activity, and the form of data request (voluntary, compulsory – transaction based, compulsory – customer account based, pop-up window).

Data collection and description. The web merchants sample is a reasoned sample (Tashakkori and Teddlie, 1998) of a hundred sites: half "pure online players" and half "bricks and clicks". They were selected on two criteria: notoriety and visit frequency (www.cybermetrie.fr).

Data was collected by browsing the web merchants' sites. Four surfers, two males and two females, all master students in Marketing & IT and experienced Internet users, worked on the data collection. Exploratory browsing of selected merchants was engaged first. This led to the deletion of some of them (closed, merged or unreachable), resulting in a final sample of 89 web merchants. Exploratory browsing was also important for the surfers as it helped to harmonize their reading of privacy and security statements. Visits were conducted in March 2003. The web merchants' characteristics are described in Table 2.

Table 2: Web merchants sample description

Sector of activity	Frequency	%
Food & drink	15	16.9
Distance selling	4	4.5
Computer & multimedia	5	5.6
Books. CD. video	21	23.6
Fashion & accessories	16	18.0
Tourism. travel	15	16.9
Health & beauty	6	6.7
Games & toys	1	1.1
Else	6	6.7
Total	89	100.0

3.2. Consumer survey

Survey instrument. The consumer questionnaire is available in appendix A. Consumers characteristics and web usage are measured through direct questions.

Three items are used to measure information privacy concern. Respondents are asked to rate on a 7-point scale whether they feel concerned about sharing their information in three different browsing situations. The standardized Cronbach alpha is .76. Hence, the average score on these items is used to assess overall information privacy concern.

Reluctance to provide personal information is measured through 15 items. Consumers indicate on a 7-point scale whether they bother to share different information such as name, e-mail, age, credit card number, family size, etc. The standardized Cronbach alpha is .84. The average score on these items is an indicator or the overall reluctance to provide personal information.

The perception of privacy and security statements is assessed through 10 items: notice aspects of privacy policies (2 items), choice dimension (3), access (1), security (2), horizon (1) and contact (1). Each item is a transposition of Culnan's studies on sites online privacy policies, except for the horizon aspect that is created for this study. Consumers are asked to rate on a 7-point scale whether they consider these statements as reassuring. The standardized Cronbach alpha is .89, indicating that items are coherent in representing consumers' perception of privacy and security statements.

Data collection and description. The consumer sample is an ad hoc sample. A total of 194 questionnaires were gathered but only 154 were retained for analysis as some of them presented incoherent patterns of response (people claiming not to surf but answering items concerning browsing). Data were collected during face-to-face interviews either at the consumer's home or at their university/college (interviews were conducted by students for their market research classroom). The sample is composed of 47.4% of student (university or college) and 52.6% from the general public. An ANOVA analysis shows there is no significant difference between students and non-students in terms of privacy concern, reluctance to provide information and perception of reassuring statements.

No specific stimulus was provided before the interview. With a proportion of 48% of males, the sample is similar to the French population in term of gender proportion (www.insee.fr). The average age is 26.95 years (std

dev.=10.29) with a minimum of 13 years and a maximum of 78 years. Consumers consider themselves as moderately expert in using the Internet (mean=3.62 on a 7-point scale, std dev=1.64). Professional characteristics of consumer sample are summarized in table 3, along with their web usage.

Table 3: Description of consumer's activity and web usage

Professional activity	Frequency	%
Farmers	5	3.2
Craftsmen. entrepreneurs	1	.6
Executives	13	8.4
Intermediary professions	27	17.5
Employees	22	14.3
Workers	3	1.9
Retired	1	.6
Unemployed	5	3.2
University students	66	42.9
College students	7	4.5
Total	150	97.4
Missing	4	2.6
Total	154	100.0
How frequently do you use Internet	Frequency	%
Occasional	69	44.8
Regular	61	39.6
intensive	23	14.9
Total	153	99.4
Missing	1	.6
Total	154	100.0
What type of Internet connection do you use?	Frequency	%
adsl	50	32.5
cable	11	7.1
56K modem	80	51.9
Total	141	91.6
Missing	13	8.4
Total	154	100.0

4. Results

4.1. Web merchant's privacy and security statements

Data Request. Commercial web sites all collect contact information, obviously. But only 41.9% of them attempt at collecting socio-demographic information such as age, family size, education, revenues, hobbies, employment or other. The form of data request is essentially compulsory (96.7%) and mainly customer-account based (60.7%) (see table 4).

Table 4: Form of Data Request

Form of data request	Frequency	%
Voluntary	2	2.2
Compulsory (transaction based)	32	36.0
Compulsory (customer account based)	54	60.7
Pop-up window	1	1.1
Total	89	100.0

Form of privacy and security statements. Only 39.3% of web merchants provide a thorough online privacy policy (table 5). But 78.6% of them go beyond the mere indication of the CNIL statements. Surprisingly, 22.5% of web merchants omit this legal, compulsory mention. Of the 85 sites developing privacy and security statements, 57.6% have a direct link from their homepage.

Detailed privacy and security statements. As indicated in table 5, privacy and security statements are often restricted to notice, choice, security, for half of web merchants. Some features are well indicated such as access

(87.6%), and contact (84.3%). However, as these two elements follow CNIL obligations.

A special mention could be awarded for statements concerning the security of financial data transmission (77.5%). This can be easily explained, as it is often one of the most sensitive issues for consumers once they have decided to buy from the site. Concerning the horizon criterion, privacy policies are still incomplete with only 6.7% of web sites indicating how long personal data will be kept and just a few more (11.2%) indicating it for financial data.

Table 5: Detailed privacy and security statements (N=89)

Detailed privacy and security statements	Yes (%)
Notice about	
-type of requested information	43.8
-use of requested information	48.3
-use of cookies	47.2
Choice	
-choice to refuse web merchant's offers	58.4
-information about dissemination	49.4
-choice to refuse offers related to information dissemination	88.6 (*)
Access	87.6
Security	
-personal data	39.3
-financial data	77.5
Contact	84.3
Horizon	
-personal data	6.7
-financial data	11.2

(*) N=44

Potential impact of the commercial structure on privacy and security statements. We tested the potential impact of the commercial structure of the company ("pure online player" or "bricks and clicks") on the thoroughness of privacy and security statements. The overall result is that there is no major difference except in two areas. Concerning notice statements, "pure online players" significantly give more information about the use of requested information ($p<0.05$). This might be understood as the need for them to increase trustworthiness of their information request. Concerning choice statements, "bricks and clicks" tend to indicate more often whether data will be divulged to other firms or partners ($p<0.05$).

4.2. Consumers' perception of web merchants' privacy and security statements

The impact of consumer's characteristics and web usage on privacy concern. In this sample, 57.2% of the consumers indicated a relatively high concern about privacy (score less than 3.5 on the 7-point scale); the average overall privacy concern is 3.30 with a standard deviation of 1.48.

Privacy concern is influenced by consumers' characteristics and web usage (table 6) as suggested in H1. Except for web usage frequency (H1d), consumer's characteristics such as gender (H1a) and age (H1b) and consumer's web usage (H1c and H1e) are all significant factors in influencing privacy concern.

The age factor has a slight, significant impact on privacy concern. As age increases, privacy concern tends to increase, except when consumers intend to buy from the web merchant. Gender is an influential variable. Females exhibit a higher overall privacy concern, especially when they simply ask for information from the web merchant ($p<.01$).

As consumer's Internet expertise grows, privacy concern is reduced which is expected as it is explained by perceived control (Hoffman, Novak and Peralta, op. cit.). The connection speed plays a role in privacy concern. Consumers with adsl or cable connection feel less concerned about privacy than those connected with 56K modems. This can be explained by the fact that experienced users are probably using high-speed connections. However, connection speed is not necessarily an important variable in all browsing situations. Connection speed does not affect privacy concern when consumer's intention is to ask for information or to buy. Thus, the impact of this variable appears to be relatively shallow. In sum, the results provide general support for H1.

Table 6: Consumers' characteristics and web usage and privacy concern

Pearson correlation		Expertise	Age
Overall privacy concern		0.25	-0.16
	Sig.	0.00	0.04
	N	143	145
Concern when browsing		0.15	-0.17
	Sig.	0.05	0.03
	N	151	153
Concern when requesting information		0.17	-0.18
	Sig.	0.03	0.02
	N	151	153
Concern when buying		0.30	-0.05
	Sig.	0.00	0.48
	N	143	145

With p= 0.05

		Overall privacy concern	Concern when browsing	Concern when requesting information	Concern when buying
male	mean	3.59		3.40	
	N	69		71	
	std dev	1.63		1.94	
female	mean	3.02		2.59	
	N	71		77	
	std dev	1.28		1.36	
Total	mean	3.30		2.98	
	N	140		148	
	std dev	1.49		1.71	
Khi²		p<.05	ns	p<.01	ns
Web usage frequency					
Khi²		ns	ns	ns	Ns
Connection speed					
adsl	Mean	3.51	3.08		
	N	47	50		
	Std dev	1.61	1.635		
cable	Mean	4.16	4.36		
	N	10	11		
	Std dev	1.68	1.85		
56k modem	Mean	3.07	2.93		
	N	76	80		
	Std dev	1.35	1.62		
Total	Mean	3.31	3.09		
	N	133	141		
	Std dev	1.491	1.67888128		
Khi²		p<.05	p<.05	ns	ns

…/…

Consumers browsing intentions and privacy concern. Consumers tend to find it normal that data are requested when browsing for buying, but surprisingly the result is not as positive as expected in the sense that the mean (3.76) is only slightly above the average theoretical value of 3.50 (table 7). However, consumers significantly differentiate privacy concern when browsing or asking information from browsing for buying (Z-test, p<.000). This is in line with previous research (Culnan and Armstrong, op. cit.; Han and Maclaurin, op. cit.) where it was found that privacy is not a concern when there is some sort of give-give situation that is perceived to be fair. Hence H2, proposing that

browsing intentions influence privacy concern, is supported.

Table 7: Consumer's intention and privacy concern

Privacy concern (*)	N	Min.	Max.	Mean	Std Dev.	Paired differences Wilcoxon Z test
(a) Data request while browsing	153	1	7	3.07	1.64	
(b) Data request when ask for information	153	1	7	3.00	1.71	
(c) Data request when buying	145	1	7	3.76	2.03	c-a & c-b : p<.000

(*) With (1): I think it's not normal to (7): I think it's normal

Privacy concern and reluctance to provide information. As shown in table 8, consumers that are mostly concerned about sharing their information are particularly reluctant to provide it to web merchants, whatever their intention: browsing, asking for information or even buying). Thus H3, stating that when privacy concern is high, the consumer will be highly reluctant to provide personal information, is supported.

Table 8: Privacy concern and reluctance to provide information

	Overall privacy concern	Concern when browsing	Concern when requesting information	Concern when buying
Overall reluctance to provide information	-0.46	-0.42	-0.38	-0.33

Correlation all significant at p<0.001

Interestingly, most of the personal data are not deemed as critical as could be expected. Disclosing civility, email, address, age, family size, gender, education, hobbies and profession is not a major problem for consumers. However, there are still some areas of information that remain personal in consumers' eyes. Name, fax number and revenue are touchy bits of information that consumers disclose carefully. Consumers are even more reluctant in disclosing credit card number (mean=6.2) and phone number (mean~5.2). This result can be linked with the fear inherent in transaction and the attitude toward direct marketing (Phelps, D'Souza and Nowak, op. cit.).

The impact of privacy concern on the perception of privacy and security statements. The results provide overall support for H4 (see table 9). This confirms that the more consumers feel concerned about privacy the more they will be demanding regarding privacy and security statements. Hence, highly concerned consumers will feel reassured by the different aspects of privacy and security statements such as notice, choice, access, security and horizon (all significant at p=.05). Nevertheless, for concerned consumers, statements regarding security about information storage and contact information are not particularly reassuring.

Table 9: The impact of privacy concern on the perception of privacy and security statements

Pearson correlation	Notic1	Notic2	Choic1	Choic2	Choic3	Access	Securi1	Securi2	Horizon	Contact
Overall privacy concern	-0.20	-0.22	-0.22	-0.25	-0.17	-0.23	-0.18	-0.15	-0.26	-0.13
Sign.	0.02	0.01	0.01	0.00	0.04	0.01	0.03	0.08	0.00	0.13
N	144.00	145.00	144.00	145.00	145.00	145.00	145.00	145.00	145.00	145.00

The hierarchy between privacy and security statements. A ranking of privacy and security statements is shown in table 10. The robustness of the hierarchy is tested with Wilcoxon Z-test, which assesses whether a mean is significantly different from another one.

Table 10: The hierarchy between reassuring privacy and security statements

Privacy and security statements (from most reassuring to least reassuring)	Mean	Paired differences Wilcoxon Z-test
		Sign p<.05
Information transmission security (security 1)	3.07	With horizon, contact, notice 1, choice 1 & 2
Choice given to share information (choice 3)	3.08	With notice 1, choice 1 & 2, horizon and contact
Access to data	3.18	With choice 1 & 2, horizon and contact
Information storage security (security 2)	3.20	Choice 1 & 2, horizon
Indication of information use (notice 2)	3.23	With : notice 1, choice 1 &2, horizon
Notice concerning data collection (notice 1)	3.45	With : notice 2, choice 1, 2 & 3, security 1, horizon
Contact	3.48	With : choice 1, 2 & 3, access, security 1, horizon
Horizon	3.78	With : notice1 & 2, choice 2 & 3, access, security 1 & 2, and contact
Choice to be re-contacted (choice 1)	3.86	With : notice 1&2, choice 2 & 3, access, security 1 & 2, contact
Notice of information sharing (choice 2)	4.24	With : notice 1&2, choice 1 & 3, access, security 1 & 2, horizon and contact

The overall hierarchy, proposed in H5, indicates that reassuring statements include "information transmission security" (3.07), "choice given to share information" (3.08), "access to own personal data" (3.18) and "information storage security" (3.20). This provides overall support for H5. Security statements as well as statements pertaining to consumer's control over information are the most reassuring. However, security statements are all not ranked before control statements. "Information transmission security" is ranked as reassuring as "choice given to share information", which indicates that even if security is claimed and guaranteed by web merchants, consumers do not want to be left passive concerning the management of their personal information. It is also interesting to observe that statements that could be judged as "advanced" privacy statements are not considered as particularly securing (horizon, choice to be re-contacted by the web site, notice of information sharing).

An examination of consumers' perception in relation with their browsing intention yields interesting results. As shown in table 11, consumers feel reassured by different privacy and security statements depending on their browsing intention.

When consumers are simply browsing, and find it normal to disclose personal information, they feel reassured by two elements: "choice to be re-contacted" and "notice of information sharing". When they ask for information from the web merchant and find it normal to disclose information, they are more demanding and will feel reassured if the web merchant indicates whether information will be shared, how information transmission will be secured and how long information will be stored. Eventually, when buying from a web site, consumers who are willing to provide information expect web merchants to develop a thorough online privacy policy, that is privacy and security statements on all aspects, with a particular emphasis on access and information use (notice 2).

5. Discussion and Implications

As consumers' perceptions are partly based upon actual web merchants' statements about privacy and security, it is important to investigate the current situation. This examination shows that a thorough online privacy policy (that is one that spans most of the privacy and security aspects) is not widespread. While consumers expect primarily "information transmission security", "choice given for information sharing", "access to personal data" and "information storage security", only 40% of web merchants develop a thorough online privacy policy. That is why, even in the French context, meeting legal requirements is not sufficient. This result indicates that there is indeed a gap between consumer expectations and the policy developed by the web merchants. This requires improvement on the part of the merchants as privacy and security statements, at appropriate times can be reassuring for the consumers. The findings of the study are summarized in table 12.

Table 11: Privacy concern, consumer's intention and perception of privacy & security statements

Privacy and security statements		Concern when browsing	Concern when asking for information	Concern when buying
Notice 1	Pearson corr.	-.102	-.112	-.266
	Sig.	.213	.169	.001
	N	152	152	144
Notice 2	Pearson corr.	-.077	-.103	-.340
	Sig.	.344	.207	.000
	N	153	153	145
Choice 1	Pearson corr.	-.191	-.141	-.207
	Sig.	.018	.084	.013
	N	152	152	144
Choice 2	Pearson corr.	-.243	-.250	-.134
	Sig.	.002	.002	.109
	N	153	153	145
Choice 3	Pearson corr.	-.147	-.058	-.205
	Sig.	.069	.480	.013
	N	153	153	145
Access	Pearson corr.	-.064	-.117	-.365
	Sig.	.430	.150	.000
	N	153	153	145
Security 1	Pearson corr.	-.048	-.171	-.248
	Sig.	.555	.035	.003
	N	153	153	145
Security 2	Pearson corr.	-.018	-.122	-.234
	Sig.	.826	.133	.005
	N	153	153	145
Horizon	Pearson corr.	-.153	-.213	-.285
	Sig.	.059	.008	.001
	N	153	153	145
Contact	Pearson corr.	-.054	-.049	-.219
	Sig.	.507	.548	.008
	N	153	153	145

Table 12: Summary of findings

Hypotheses and research question	Result	Finding
H1 Role of consumer characteristics on privacy concern	General support	H1a (age) +/sign. H1b (gender) +/sign. H1c (expertise) +/sign. H1d (frequency) ns H1e (connection) +/sign.
H2 Role of consumer intention on privacy concern	Overall support	Buying intention > browsing at will or asking for information
H3 role of privacy concern in reluctance to provide information	Support	High privacy concern generates reluctance to provide information
H4 role of privacy concern on the perception of reassuring privacy & security statements	Overall support	highly concerned consumers will feel reassured by the different aspects of privacy and security statements
H5 hierarchy between reassuring statements	Overall support	Security and control statements are the most reassuring. Note: perception of reassuring statements vary according to consumer intention
Research question: web merchants' privacy and security statements	- The main form of data request is compulsory (96%) - Only 39.3% of web merchants provide thorough privacy and security statements.	

From a theoretical standpoint, although previous research (such as Pavlou and Chellappa, op. cit.; Belanger et al., op. cit.) showed that privacy statements are not heavy predictors of online trust, a potential explanation might lie in the fact that web merchants' online privacy policies are still insufficiently detailed. Indeed, Gurau, Ranchhod and Gauzente (op. cit.) found that only 15% of US e-tailers provide privacy charts. Once the situation has been improved this could change. So the role of privacy and security statements is still an important issue for research. It is necessary to investigate how these statements can become efficient trust busters. The present study contributes to the differentiation of reassuring statements, which could lead to new practices. It finds that highly concerned consumers expect web merchants to indicate clearly how information security and control are guaranteed. Further investigation is now needed to reassess the role of privacy and security statements. Experiments would be of high value in order to re-evaluate the respective role of *detailed* privacy and security statements, including those that are perceived to be of highest value by consumers, and the role of other sites' features in trust building. A detailed review of these would enable researchers to understand their impact on consumers (perceived security/trust)

Another theoretical contribution of the study is to underline that like consumption, privacy concern is not only a matter of individual characteristics (which has been already showed in previous studies) but that it is also a matter of situation. Privacy concern could be considered as a multidimensional construct entailing a core concern (the tendency to feel concerned) and peripheral aspects, which will vary according consumption situations and consumer's intentions.

From a managerial viewpoint, the results suggest web merchants should implement thorough privacy and security statements and present them in a policy or chart. Policies should primarily underline how information security and consumer control over information are guaranteed. The study also suggests that in order to reduce consumers' reluctance to provide information (which remains a matter for 60% of consumers) web merchants should tailor their privacy and security statements according to consumers' browsing intention. For instance, when consumers ask for information a dynamic link should be generated to a page where the policy underlines statements that are of prime importance at this stage of the relationship (that is "information sharing", "information transmission security" and "information storage horizon"). Similarly, when a consumer places an order another type of link should be generated where the overall policy is presented with an emphasis on "access to information" and "use of information".

In addition, the study indicates the type of personal information that is considered to be private. This can help web merchants to behave in a non-intrusive manner and to avoid asking unnecessary information especially in the early stages of the relationship. A privacy concern continuum can be schematized as shown in figure 2.

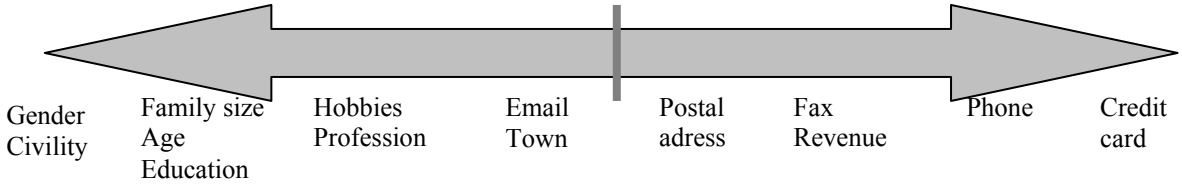

Figure 2: The privacy concern continuum

6. Limitations and Future Research

This exploratory study naturally has some limitations. The first one pertains to the respondent sample. It is possible that people who decided to answer the questionnaire were not representative of highly concerned consumers. Indeed, highly privacy concerned consumers may have refused to answer the questionnaire, introducing a bias. This potential bias is reduced, as the questionnaire was answered anonymously. There may also be a small bias, because of the sample skew towards students at around 50%. However, this may be reasonable as 35.9% of the French surfers are between 11 and 24 years of age (Mediametrie-Insee, March 2004), and one would expect a higher proportion of teenagers to be surfers.

Another limitation relates to the administration of the questionnaire. The questionnaire was administered off-line, with no stimulus. It is possible that different answers might have been obtained if consumers had been interviewed while browsing. Therefore, additional research is needed using, for instance, experience settings in order to grasp more precisely the impact of each dimensions and consumers' reactions toward privacy security statements.

A last limitation relates to the cultural context of the study. Milberg et al. (op. cit.) observe a U-shaped relationship between nationality and privacy concern. In particular, people from countries where privacy is highly government-regulated tend to be less concerned about privacy. If this were true, the generalizability of our results

would be limited to other highly regulated countries. However, the results indicate that our consumers' sample exhibits an average concern that is relatively high (3.30 on a 7-point scale) with reasonable deviation (1.48). Hence, the conclusions of this study can be reasonably transposed outside of France.

Concerning future research directions, although certain privacy and security statements do not appear to be particularly reassuring, their absence might compromise consumers' trust. It would be then interesting to assess in a comparative study the impact of the absence of certain statements.

The present study does not look at features such as brand reputation, a site's pleasant features, seals and trusted third parties' role, that also influence the formation of trust. Future research should try to assess the relative predictive power of each of these features along with *detailed* privacy and security statements.

Concerning clicks and bricks merchants, it would be interesting to further investigate the interaction between their online statements and their privacy policy in «real world» environment, as Hoffman, Novak and Peralta (op. cit.) underlined that privacy concern is highest in computer-mediated environment.

A «dyadic» designed research could also help in grasping more precisely consumers' perception of privacy protection when confronted to a specific web merchant. In this line, it would be important to go beyond multi sectoral studies, such as the present one, and to investigate sector specificity as different products create differing results on privacy and consumer involvement.

7. Conclusion

The present study was aimed at bringing additional understanding of consumer privacy perception. The advocated model suggests that privacy perception is a function of the web merchant's statements and consumer's perceptions. Based on this, the empirical study investigated two samples. Although they live in a government-regulated country, French consumers appear to be very concerned with data protection. At the same time, web merchants do not necessarily implement thorough privacy policies. It is suggested that web merchants go beyond legal requirements in order to establish trust with their current and potential consumers. Taking into account that issues surrounding privacy depend on consumer needs and desires, web merchants should try to adapt the way they present their privacy and security statements as well as their information requests. The potential benefits are numerous. The relationship, in the early stages, will be perceived as less intrusive if unnecessary information is not asked for and if appropriate privacy and security statements are presented to potential consumers. This should contribute to consumer's trust in a progressive manner. As trust takes time to build, progressive stages of interaction and permission to gather information, should contribute to the overall quality of the relationship. A good customized privacy policy can lead to a trusting and durable relationship, with the potential for repeat purchase and the development of loyalty (Brown and Muchira, 2004).

Acknowledgements

The author thanks the three JECR reviewers for their helpful comments. The authors is also grateful to Pr. A. Ranchhod, Southampton Business School (UK) for his help and comments on the second version of this text.

REFERENCES

Ang, P.H., "The Role of Self-Regulation of Privacy and the Internet", Journal of Interactive advertising, Vol. 1, N°2, [accessed April 2003], 2001.

Barwise, P. and C. Strong, "Permission-based Mobile Advertising", Journal of Interactive Marketing, Vol. 16 N°1: 14-24, 2002.

Belanger F., J.S. Hiller and W.J. Smith, "Trustworthiness in Electronic Commerce: The Role of Privacy, Security and Site Attributes", Journal of Strategic Information Systems, Vol. 11: 245-270, 2002.

Brown, M. and R. Muchira, "Investigating the Relationship between Internet Privacy Concern and Online Purchase Behavior", Journal of Electronic Commerce Research, Vol. 5, N°1: 62-70, 2004.

Caudill, E.M. and P.E. Murphy, "Consumer Online Privacy : Legal and Ethical Issues", Journal of Public Policy & Marketing, Vol. 19, N°1: 7-19, 2000.

CNIL. www.cnil.fr/uk/cnil/about.htm [accessed June 2003]

Corbitt B.J., T. Thanasankit and H. Yi, "Trust and E-Commerce: A Study of Consumer Perception", Electronic Commerce Research and Application, Vol. 2: 203-215, 2003.

Culnan, M. J. and P.K. Armstrong, "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation", Organization Science, Vol. 10, N°1: 104-114, 1999.

Culnan, M.J. and G.R. Milne, "The Culnan-Milne Survey on Consumers & Online Privacy Notices : Summary of Responses", Federal Trade Commission. http://ww.ftc.org/bcp/workshops/glb/supporting/culnan-milne.pdf [Accessed June 2003], 2001.

Culnan, M.J., "Privacy and the Top 100 Web Sites : Report to the Federal Trade Commission", http://www.msb.edu/faculty/culnanm/gippshome.html [Accessed : December 2001], 1999a.

Culnan, M.J., Georgetown Internet Privacy Policy Survey : Report to the Federal Trade Commission, http://www.msb.edu/faculty/culnanm/gippshome.html [Accessed : December 2001], 1999b.

Dommeyer, C.J. and B.L. Gross, "What Consumer Know and What They Do : An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies", Journal of Interactive Marketing, Vol. 17, N°2: 34-51, 2003.

Evans, M., "The Relational Oxymoron and Personalisation Pragmatism, Journal of Consumer Marketing, Vol. 20, N°7: 665-685, 2003.

Gauzente, C. and A. Ranchhod, "Ethical Marketing for Competitiveness on the Internet",. Academy of Marketing Science Review, Vol. 10, N°1, http://www.amsreview.org/articles/gauzente10-2001.pdf [Accessed March 2003], 2001.

Gauzente, C., "Vie privée et Internet : Les pratiques des sites français", Décisions Marketing, Vol. 30: 1-10, 2003.

Gillin, D., "The Federal Trade Commission and Internet Privacy", Marketing Research, 39-41, Fall 2000.

Godin, S., Permission Marketing, New York: Simon & Schuster, 1999.

Grabner-Kräuter, S. and E.A. Kaluscha, "Empirical Research in On-line Trust: A Review and Critical Assessment", International Journal of Human-Computer Studies, Vol. 58: 783-812, 2003.

Gurau, C., A. Ranchhod and C. Gauzente, "To Legislate or not to Legislate": A Comparative Study of Privacy/Personalisation Factors Affecting French, UK and US Web Sites", Journal of Consumer Marketing, Vol. 20, N°7: 652-664, 2003.

Han, P. and A. Maclaurin, "Do Consumers really Care about Online Privacy ?", Marketing Management, 35-38, 2000 January/February

Hoffman, D.L., T.P. Novak and A. Schlosser, "Consumer Control in Online Environment", Elab.vanderbilt.edu, February 25 2000.

Hoffman, D.L., T.P. Novak and M. Peralta, "Building Consumer Trust Online Communication to the ACM", Vol. 42, N°4: 80-85, 1999a.

Hoffman, D.L., T.P. Novak and M.A. Peralta (1999b), "Information Privacy in the Marketspace : Implication for the Commercial Uses of Anonymity on the Web", The Information Society, Vol. 15, N°2: 129-140, 1999b.

INSEE: www.insee.fr [accessed May 2003]

Jarvenpaa S.L., N. Tractinsky and L. Saarinen, "Consumer Trust in an Internet Store: A Cross-Cultural Validation", Journal of Computer-Mediated Communication, Vol. 5, N°2, online http://www.ascusc.org/jcmc/ [accessed December 2003], 1999.

Johnson J.L., A Theory of the Nature and Value of Privacy, Public Affairs Quarterly, Vol. 6, N°3: 271-288, 1992.

Kelly, E.P. and H.C. Rowland, "Ethical and Online Privacy Issues in Electronic Commerce", Business Horizons, Vol. 43, N°3: 3-12, 2000.

Lim N., "Consumers' Perceived Risk : Sources versus Consequences", Electronic Commerce Research and Application, Vol. 2: 216-228, 2003.

Luo X., "Trust Production and Privacy Concerns on the Internet, A Framework Based on Relationship Marketing and Social Exchange Theory", Industrial Marketing Management, Vol. 31: 111-118, 2002.

Mabley, K., "Privacy vs. Personalization", Cyber Dialogue, www.cyberdialogue.com/library/ pdfs/wp-cd-2000-privacy.pdf, [accessed June 2003], 2000.

Mason, R.O., "Applying Ethics to Information Technology Issues", Communication of the ACM, Vol. 38, N°12: 55-57, 1995.

Milberg S., S. Burke, J. Smith and E. Kallman, "Values, Personal Informations, Privacy and Regulatory Approaches", Communications to the ACM, Vol. 38: 65-74, 1995.

Miyazaki, A.D. and A. Fernandez, "Consumer Perception of Privacy and Security Risks for Online Shopping, The Journal of Consumer Affairs, Vol. 35, N°1: 27-44, 2001.

Nowak, G.J. and J. Phelps, "Understanding Privacy Concerns", Journal of Direct Marketing, Vol. 6, N°4: 28-39, 1992.

Nugent, J.H. and M.S. Raisinghani, "The Information Technology and Telecommunications Security Imperative : Important Issues and Drivers", Journal of Electronic Commerce Research, Vol. 3, N°1: 1-14, 2002.

Palmer J.W., J.P. Bailey and S. Faraj, "The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements", Journal of Computer-Mediated Communication, Vol. 5, N°3 [online : http://www.ascusc.org/jcmc/], 2000.

Pavlou, P.A. and R.K. Chellappa (2001), "The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transaction", Ebizlab Working paper, 39 p., January 2001.

Phelps, J.E., G. D'Souza and G.J. Nowak, "Antecedent and Consequences of Consumer Privacy Concerns : An Empirical examination", Journal of Interactive Marketing, Vol. 15, N°4: 2-17, 2001.
Roznowski, J.L., "A Content Analysis of Mass Media Stories Surrounding the Consumer Privacy Issue 1990-2001", Journal of Interactive Marketing, Vol. 17, N°2: 52-69, 2003.
Schoenbachler, D.D. and G.L. Gordon, "Trust and Customer Willingness to Provide information in Data-driven Relationship Marketing", Journal of Interactive Marketing, Vol. 16, N°3: 2-16., 2002.
Shankar V., G.L. Urban and F. Sultan, "Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions", Journal of Strategic Information Systems, Vol. 11: 325-344, 2002.
Shin, N., "Strategies for Competitive Advantage in Electronic Commerce", Journal of Electronic Commerce Research, Vol. 2, N°4: 164-171, 2001.
Solove, D.J., "Conceptualizing Privacy", California Law Review, Vol. 90: 1087-1155, 2002.
Sultan, F., G.L. Urban, V. Shankar and I.Y. Bart, "Determinants and Role of Trust in E-Business: A Large Scale Empirical Study, MIT Sloan School of Management Working paper, 4282-02, 2002.
Tashakkori A. and C. Teddlie, Mixed Methodology, Combining Qualitative and Quantitative Approaches, Sage Publications, 1998.
Teltzrow, M. and A. Kobsa, "Impact of User Privacy Preferences on Personalized Systems – A Comparative Study", CHI'03 Conference, 2003.
Tezinde, T., B. Smith and J. Murphy, "Getting Permission : Exploring the Factors Affecting Permission Marketing", Journal of Interactive Marketing, Vol.16, N°4: 28-36, 2002.
Yoon, S.J., "The Antecedents and Consequences of Trust in Online-Purchase Decisions", Journal of Interactive Marketing, Vol.16, N° 2: 47-63, 2002.

APPENDIX A. CONSUMER QUESTIONNAIRE (TRANSLATION FROM FRENCH)

Consumer characteristics

Age Gender Activity

Frequency: How would you describe your web usage ?
(1) Occasional / (2) regular / (3) intensive

Expertise: How would you describe your web expertise ? 7-point scale
(1) beginner to (7) expert

Connection: What type of Internet connection do you generally use ?
(1) ADSL
(2) cable
(3) 56K modem

Information privacy concern

1. Do you think it is (1) completely not normal → (7) completely normal that personal information are required from you while simply browsing on the Internet ?
2. Do you think it is (1) completely not normal → (7) completely normal that personal information are required from you when you ask information from a web merchants ?
3. Do you think it is (1) completely not normal → (7) completely normal that personal information are required from you when you buy from a web merchant ?

→ Overall Information Privacy concern is the score on all 3 items

Reluctance to provide personal information

In general, does it bother you to provide the following information (1) not at all → (7) very much?

1. Title
2. Name
3. Email address
4. Postal address
5. Telephone number
6. Fax number
7. Credit card information
8. Age/date of birth
9. Family size
10. Gender
11. Education
12. Town
13. Revenue
14. Hobbies
15. Profession

→ Overall Reluctance to provide personal information is the average score on all 15 items

Reassuring Elements of Online Privacy and Security Statements
Do you consider the following web merchants' statements as reassuring ?
(1) Absolutely yes → (7) Absolutely not

Notice
1. The fact that the web merchant indicates which data are collected and how they are collected.
2. The fact that the web merchant describes how data will be used.

Choice
1. The fact that the web merchant gives you the choice to be re-contacted later.
2. The fact that the web merchant indicates you whether data will be shared with third parties.
3. The fact that the web merchant asks your authorization to share your information with third parties.

Access
- The fact that the web merchant describes how you can modify your personal information.

Security
1. The fact that the web merchant explains how your information is secured during their transmission.
2. The fact that the web merchant indicates which means are used in order to protect your data while storing.

Horizon
- The fact that the web merchant indicates you how long your data will be stored.

Contact
- The fact that the web merchant indicates who you can contact for privacy matters.