

e-Marketing and privacy legislation: mind the gap.

Evaluation of online privacy statements in respect to the European dataprotection directive (95/46/EC) and the Belgian privacy law (8/12/92 and 11/12/98).

Michel Walrave

e-Marketing and privacy legislation: mind the gap.

Evaluation of online privacy statements in respect to the European dataprotection directive (95/46/EC) and the Belgian privacy law (8/12/92 and 11/12/98).

Abstract

The use of different forms of marketing communications on the internet is definitely on the rise. During those interactive communication processes, personal data are often collected not only in an explicit manner (f.e. using electronic forms), but in an implicit manner as well (f.e. using cookies, clickstream analysis). The collection and use of data of internet users for marketing purposes raises questions concerning the protection of the consumers' online privacy. To protect the *informational* privacy (i.e. dataprotection) and the *relational* privacy (i.e. in this domain the right not to be contacted by companies for marketing purposes) legislative initiatives have been taken in the European Union. From an analysis of 250 Belgian websites it results that the majority, collecting personal data, score largely unsatisfactorily concerning the information towards the consumer, as imposed by the European dataprotection directive transposed in the Belgian privacy law. This first analysis of websites in march 2001 (before the new privacy law came into effect on september 1st) and a second analysis, one year later, in april 2002 forms part of series researches about e-privacy, the protection of internet users' privacy. In this paper, the results of an analysis of Belgian websites are also compared with research in other countries.

Extracto

Protección de la privacidad en sitios web: examen de cómo se aplica la legislación existente sobre protección de datos privados en los sitios web belgas.

El uso de diferentes formas de marketing directo en internet va en aumento. En este proceso interactivo de comunicación, los datos privados no sólo se recopilan de forma explícita (por ejemplo en formularios electrónicos), sino también de forma implícita (por ejemplo por medio de *cookies*, análisis de flujo de clics, etc.). La recopilación y el uso de los datos privados de los usuarios de sitios web que el marketing directo lleva a cabo suscitan dudas sobre la seguridad en las relaciones y los contactos en la red. Es necesario que surjan diferentes iniciativas legislativas tanto a escala nacional como europea para proteger la privacidad *informativa* (es la protección de datos privados) y la privacidad *relacional* (en este contexto, el derecho del consumidor a elegir si una empresa puede contactar con él con fines comerciales). Un estudio de 250 sitios web belgas que recopilaban datos privados refleja que la mayoría de las empresas violan el derecho a la intimidad de las personas que confían sus datos privados, infringiendo las directrices europeas y la legislación vigente en Bélgica. Este primer análisis de sitios web de marzo de 2001 (anterior a la nueva ley belga de 1 de septiembre de 2001) y un segundo análisis el año siguiente (en abril de 2002) forman parte de una serie de estudios sobre la protección de la 'e-privacy', la vida privada en internet. En esta charla trataremos de comparar nuestros resultados con los resultados de investigaciones en otros países.

Author

Prof. dr. Michel Walrave is attached to the Catholic University of Leuven (K.U. Leuven), the University of Antwerp and guest lecturer at the Universidad Ramon Llull Barcelona. He conducts research, publishes and teaches about marketing communication, direct marketing, call centres, e-marketing and the protection of the consumer's privacy. He works as an advisor for different institutions concerning privacy policy. He is member of the editorial board of The Journal of Consumer Behaviour and the R.P.O.T (Belgian Privacy Journal). He is a member of the FiuCom board (International Federation of Catholic Universities, section of communication sciences).

address: Department of Communication Science K.U.Leuven,
Van Evenstraat 2A, B-3000 Leuven, Belgium.

telephone: + 32 16 32 32 29 fax: + 32 16 32 33 12

e-mail: Michel.Walrave@soc.kuleuven.ac.be

e-Marketing and privacy legislation: mind the gap.

Evaluation of online privacy statements in respect to the European dataprotection directive (95/46/EC) and the Belgian privacy law (8/12/92 and 11/12/98).

1. Introduction

Thanks to the unique characteristics of the internet, businesses can contact prospects and clients and inform them about products and services using multimedia and interactive communication processes. This commercial communication is not only possible by using banners and intermercials (i.e. internet commercials), but also personally and in an interactive manner by e-mail, chat and by other applications of the internet technology. When a company communicates online with a consumer, personal data are very often collected. In this case we enter the delicate domain of individuals' privacy. When we are talking about privacy, we make a distinction between informational and relational privacy.

The *relational privacy* of a person, in the context of direct marketing in general and of e-commerce in particular, is the degree of disponibility of the consumer to be reachable by organisations. In other words, the answer to the questions if, when and how the consumer wants to communicate directly with an organisation. This liberty to decide with which organisations a consumer is willing to keep up contacts and by which media, can be respected by inter alia the Robinson lists, ethical codes, specific legislation and newly designed technology. Respect for the relational privacy means that the consumer is given the chance to protect him- or herself from certain expressions of direct marketing communication, but also to inform a business which types of communication are welcome. This forms also a key aspect of the debate concerning *opt-in* (giving explicit permission to use data for direct marketing purposes using e-mail for example) versus *opt-out* (the right to oppose against the use of one's e-mailaddress, for example, for direct marketing).

Informational privacy concerns the possibility of a person to control his or her personal data. In other words, the consumer receives the possibility to take an informed decision when an organisation asks him or her to communicate personal data. This supposes *transparency* in the purposes of the gathering, processing and commercialising of consumers' information. This transparency, being one of the cornerstones of the dataprotection legislation, must be translated in specific and complete information at the moment of collecting personal data among the consumers, not only for example in reply coupons and forms, but also during conversations with call center agents and when filling in an electronic forms on a website. This information and promise to use personal data respectfully and lawfully, is formulated in a *privacy statement* which has to be a part of a website for example. But even a privacy promise is debt. It would be better that this is not a façade, but a concrete expression of the mentality in the organisation, which is in touch with the respect for the personal data of prospects and clients (cfr. Westin: 1991; Walrave: 1999).

This privacy promise has to rest on an existing legislation which imposes a number of obligations to persons and organisations processing data about individuals. In Belgium the protection of the informational privacy is regulated by the law that converts the directive 95/46/EC of 24 October 1995 of the European Parliament and the Council concerning the protection of natural persons in relation with the processing of personal data and concerning free movement of those data (law of 11 December 1998, published on 3 February 1999). This 'privacy law', as she is called in short, brings the original Belgian law (of 8 December 1992) in conformity with the regulations of the European data protection directive (95/46/EC). A number of discrepancies between the original Belgian law and the directive, have obliged the

Belgian legislator to revise the law and certain supplementary rights had to be given to the individuals among other changes to the national law.

Besides the privacy law, there are other national laws and European directives regulating aspects of the protection of the informational and relational privacy. Here we narrow down the scope of this research to the application of the principles of the dataprotection directive, transposed in the national privacy law, in Belgian websites. We will investigate in how far the duties imposed by the law are respected in commercial websites. Actually we will look in what measure and how those rights and other information about the processing of personal data on the website, are dealt with in for instance a privacy statement. We will not only check how many websites are communicating the necessary information, but also how complete that information is and in what way it is communicated.

In this research we will analyse the degree of respect for informational privacy. The relational privacy is herewith closely linked in the domain of the online direct marketing. For instance, if a company offers the possibility to the consumer not to let his data being processed for direct marketing, than in this concrete case the relational privacy of that consumer is also protected. Namely, he or she does not receive any e-mailings, eventually no telemarketing calls and direct mails from that firm. But we will also check if websites integrate an opt-out or opt-in when they are collecting e-mail addresses for marketing purposes.

Before we go into what degree and how data about internet users are collected in Belgian websites, we have to specify that there are two ways of collecting data about individuals on the internet: an explicit and an implicit way. Explicit concerns the free and conscious communication of information by the internet user in electronic forms. Thus, when an internet user completes an electronic orderform, a coupon to receive information about products and services and so on. In this case the visitor of a website has a certain control about what data are communicated to which business or organisation. With the implicit collection of data this is more difficult. Implicit data are generated during a surfing session, often without the knowledge of the visitor of that website, purely by the handling of the internet technology. These data are analysed by a growing number of webmining companies using this information as basis for research, prospecting and segmented webvertising (such as banners) or one-to-one marketing. Each internet user leaves traces on the information highway, and very often the internaut is not aware of these traces. The use and analysis of these traces is sometimes called 'click stream analysis', when each click, each movement and decision of an internet user can be followed and draw in details his or her internaut profile. A growing number of software is designed, sometimes referred to as 'spyware' or when connected to marketing or advertising purposes 'adware', to build that knowledge about individual online consumers. Linking the explicit collected data and the implicit traces is a strong marketing instrument, that becomes also a big challenge towards the protection of the privacy of the online consumer.

In this research we will mainly look for what data are collected the explicit way, how this occurs concretely and if this is in conformity with the existing legislation. We will analyse also one implicit way of data gathering, namely by using cookies. A cookie consists of an information string that is automatically sent by the webserver to a client-machine (the users' PC) and stored on the harddisk of that computer when the user visits a website (or opens an e-mail). The browser creates a file where all the cookies will be stored. Such a file contains among others the name of the cookie, the value of the cookie (can be a unique code), the date of expiry (end of surfing session or sometimes a remote date) and the domain name (and directory) where the cookie (at a future session) can be sent¹. The cookie stays on the computer (till the user deletes it or untill the deadline is reached) and is communicated to the server when he or she visits that website again. We want to stress that a cookie does not in itself identify an individual, but it identifies a computer that stocked the cookie. To link

surfing behaviour with an individual, one must combine the information generated by the cookie with the identity and possibly other personal data of a website visitor. By him- or herself the user stays anonymous unless the website visitor entered personal data in an electronic form of the website he or she visits, or another website that commercializes this information, and that these data are for example connected to a unique code stored in that cookie. Every time a visitor returns to the website, his/her browser will send that cookie to the server and the server will recognise the computer by that cookie, that acts as a *barcode*. In this situation, cookies can have a commercial function: they can track the clickstream of the user; in this way the website can see in what information (products/services) the client is interested and so offer novelties during a future visit. Also the key-words used by the visitor in the search engine can be stocked and refine the visitor's profile. As long as a user does not identify him- or herself by name and other personal data and as long as these unique personal data are not linked to the cookie, the server can not know what individual has been on the website. One knows only that a user of that computer (where the cookie is stored) has already visited the website, what pages have been consulted, in what language, among other things.

Originally cookies were only meant as time-savers. A cookie can accelerate and facilitate the consultation of information at a next visit of an internet user, because some data in a form are automatically completed from a second visit on. A widely used function of cookies, and particularly useful for website visitors, consists of at a second visit automatically calling the language chosen at the first visit. This is possible because the server recognises the language chosen during his or her initial visit, stored in the cookie. Also the completion of forms can be made easier by a cookie, because the server fills automatically the form in (of a caddie in an e-shop, for instance) with the personal data as a specific visitor is recognised. In a word, the surfing can accelerate and be easier with a cookie. As explained earlier, cookies offer also marketers the possibility to track internet users' visits, record the webpages selected and by doing so, know what individual visitors like or dislike. This helps e-marketers to build profiles and to send offers that fit a specific profile, by a pop-up commercial while surfing or a banner ad (i.e. an electronic advertising poster) or an e-mailing (an electronic direct mail). For this last purpose, the cookies stocked on the computer must be linked to personal data (at least an e-mail address) communicated explicitly in the website or in another website that hires or sells this information.

Browsers though give the internet user the possibility to control or even stop this clandestine chatting between his or her computer and the website's server. One can block the venue of cookies or ask more information about the cookie before accepting or rejecting it. But till now accepting cookies is the default option. Moreover, surfing can become difficult, sometimes even impossible if an internaut does not accept cookies. That is why software is created to protect online privacy from cookies and other online spying, called P.E.T.'s, privacy enhancing technologies².

If cookies are linked to personal data and if the surfing behaviour is tracked individually, without that the concerned person knows about it nor that he or she can stop that analysis, then we can call this activity a violation of the informational privacy. For this reason we will verify in our analysis of online data collection also if the websites using cookies inform their visitors about that fact and grant them specific rights and options concerning this implicit gathering of data.

2. Methodology: selection of websites

All together about 250 websites have been analysed in detail with a standardised form testing 93 items. These items rest on the one hand on legislation and self-regulation, on advice from the Belgian Privacy Commission and on the other on a certain number of quality criteria that

we found representative for a transparent and honest processing of personal data on websites (cfr. Thomas, 2001; Walrave, 1999; Walrave, 2001b). How did we select those websites? As there is no complete and reliable list of all commercial websites from Belgian companies available, we had to start our experimental sampling off line. We consulted the official databank of Belgian businesses and made a list at random from the different NACE categories. The following step consisted to verify one by one if the selected businesses had really a website. More precisely, it had to be a website in at least one of the three national languages and/or English and aimed at a consumers' public. The pure business-to-business companies were not included in the sample. Among all the chosen websites some had to be discarded as their website was not accessible any more at the moment of the analysis. Finally, 250 websites of firms, that fulfilled our criteria were chosen to take part³. We preferred this method of selection above a random access by search engines or above a selection through online indexes or webguides, because these lists of websites can be influenced by advertising contracts and affiliation marketing practices. Considering there is no way to know the total number of websites of the businesses established in Belgium, we certainly can not pretend to aim at a representativity. Although, the used method guarantees a distribution of the tested items over the different economical sectors. In the full research report, the results are illustrated with some examples (cfr. Walrave, 2001a and Walrave, 2002). In this paper we give a synthesis of the results of the first analysis in 2001, but also the first results of our second analysis of the same sample in 2002⁴. We want to use our research instrument to conduct a longitudinal and possibly comparative research. By repeating the same analysis of the same sample of websites after the new privacy law came into effect (but also again in the future), we want to measure the possible changes in the online privacy policies (i.e. the longitudinal aspect of the research). Moreover we plan to use our online questionnaire to measure different aspects of the privacy statements in corporate en commercial websites of other countries (i.e. the comparative aspect of the research) and to focus the analysis on specific sectors or target groups (for example, a research will be conducted on kid's online privacy). Finally we want to stress that Belgium will normaly in 2002 adopt the opting-in regime for e-mailmarketing and SMS-advertising. In our research we already measure the number and characteristics of the opting-out or the opting-in procedures that already figure in electronic forms. After this new Belgian law will come into effect, a specific evaluation of the implementation of the opting-in rule will be conducted.

In this paper we look for the answer on following questions: How many websites are collecting personal data? What kind of personal data are processed? To what degree the rights of the consumer are respected? How are those rights communicated? Are website responsables able to answer a simple question (asked in a mystery e-mail) concerning their privacy policy?

3. Results: scanning the websites

3.1. How and which data are collected?

Concerning the explicit collection of data we have observed that 93% of the visited websites ask in one way or another personal data of their visitors: by means of an electronic form or a subscription to an e-zine, an orderform, a guestbook or a form to ask more information about products and services (in 2002 this is the case of 90,5% of the sample, which is not a significant difference). Also the possibility to e-mail to the webmaster or to the customer service is considered to be a processing of personal data, as the company obtains the e-mail address (and eventually co-ordinates and other information put in the message by the author him- or herself). Actually the data are gathered in the following ways:

	2001	2002
Only an electronic form	34%	43%
Only an orderform	9%	14%
Only feedback through e-mail	9%	3%
Different types of forms	48%	39%

Table 1: Methods of gathering data online.

After the question if personal data are really collected online on the Belgian commercial websites, it is interesting to verify which data are asked the most or the least on a website. In 96% of the cases the e-mail address has been asked. Some websites that collect information online (namely only 4%) seem to ask personal data but not the e-mail address. The other data asked are reproduced in Table 2, with their respective frequency. We observe a significant decrease of the processing of some types of personal data. If this is a trend in general or in specific types of websites, sectors or companies will be studied in more details in a follow-up research.

It is conspicuous that the residual category is extensive. Under this type of personal data we mention mainly: language, country, nationality, gender, own website address, name of employer. Sometimes information is asked about familial situation (number of members, marital status) or space is provided to formulate remarks and wishes concerning the contents and the outlook of the website. A few websites that are aimed at persons under age ask data of their parents, without mentioning the privacy guarantees. Several websites go even further, namely questions are asked about spare time and lifestyle. In this last category, personal data are asked considered as 'sensitive data' by the privacy law and subject to very strict rules (prohibition of processing these data, with a few exceptions). Although these data are asked for, the website does not provide any information about the privacy rights and the purpose of the data processing. Even the specific rules to process sensitive data are not respected.

	2001	2002
Name	98%	84%
Address	90%	77%
Telephone	82%	69%
GSM	10%	14%
e-Mail	96%	85%
Studies	7%	7%
Profession	22%	18%
Date of birth	25%	28%
Other data	34%	41%

Table 2: Which data are collected online.

An item, that has been examined during this analysis, was if on the electronic form a difference has been made between necessary information and secondary data. It was notable that some websites collect data that are strictly irrelevant for the explicitly mentioned goal of the processing. An example: to obtain a free subscription of an e-zine, only the e-mail address is necessary. But we noticed that several organisations link that subscription to a (sometimes compulsory) filling in of other personal data. These secondary data can be an interesting source of information about the website visitors and can also be used to maintain segmented contacts with interested consumers. Those additional goals must be explicitly mentioned. The

consumer must have the choice to communicate or not additional information. Finally, the consumer must receive some control over the administration and the use of his or her data. In 2001 only 46% made, in their list of data, the difference between necessary data and data that are facultative. In 2002 we observe a significant increase of this fundamental choice that is given to the website visitor. 56 % of the electronic forms make this difference clear.

3.2. Is a privacy statement present?

When data are collected (online), the person who is responsible for that processing must give the following information to the concerned people, in respect to the revised Belgian privacy law, namely: who is the responsible person for this processing and the address of the person or organisation, what is the purpose or different purposes of that processing, how a person can oppose oneself, without charge and without giving the reason, against the processing of his/her data for direct marketing (according the new privacy law) and also if the dataprocessing is compulsory and what are the consequences if all or some data lack. Taking into account the specific circumstances of the collection of the data, additional information can be communicated, for instance: who are the receivers (or categories of receivers) of the data, if these data are not (only) used by the organisation that collects them, but sold or hired to others. At last they can also point out that there exists a right of access and of correction of the own personal data. Those last three pieces of information have not to be communicated if they do not seem necessary, in the given circumstances, to guarantee an honest processing of the personal data with respect to the concerned people. For instance, if an organisation gathers data for a third, then in all fairness that third has to be identified.

These are, in a nutshell, the minimal informations to be given to a person when communicating his or her personal data. But, when and where must this information be given in the best way? The law suggests that the concerned person must be informed the latest when the data are obtained. On a website it will be just before filling in an electronic (order)form. Ideally this information should be assembled in a *privacy statement*, that is displayed at the top of that form. Also a few words (f.e. Privacy Policy) or a symbol can be put on top of a form that is linked to the privacy statement, that could appear in a pop-up window. The privacy law precises also that the right of opposition, in the case of direct marketing, has to be granted on the form where data is written down, using for example a simple sentence with a tick-box.

The central question that we are asking in this research is indeed: is the consumer informed about the privacy policy of the firm? This global question falls apart in several subdivisions: Which privacy rights and other legally obliged information is mentioned or not? Where is this mentioned? Has the privacy statement a separate place on the website or is it part of a general customer policy page or disclaimer? And by no means the least important is that the consumer is also informed about the procedure to follow in case of, for instance, the application of his right of access, correction or opposition.

In the studied websites collecting personal data, we found during our analysis in 2001 a privacy statement on 43% of the sample of websites. So, not even half of the websites collecting explicitly personal data have somewhere on their site formulated a text, where the information imposed by the privacy law can be found, although the original privacy law came in force in 1993. We observe that the visited web-shops score better in this matter than the corporate websites of businesses. 54% of the e-shops give information about their privacy policy against only 40% of the corporate websites. The privacy statement of the e-shops is often closely linked with other information, that a webshopkeeper must give according the Belgian law concerning trading practices, for instance. Our second analysis of the research sample in 2002 indicates a significant increase of this number. 55% have put their privacy

policy online. Again the webshops score better than the corporate websites. 61 % of the e-shops put a privacy statement online, compared to 55 % of the corporate websites (other categories of websites, f.e. portals, e-zines not included).

The companies having such a privacy statement, do they give her a place of honour on a separate webpage or is that privacy policy part of a wider policy where among other things the consumer's rights are enumerated? 47% dedicates a separate page to it (60% in 2002). This privacy statement is a synthesis of the organisation's privacy policy, in which information is given about the organisation collecting and using the data, the goals of the dataprocessing and the rights of the persons who entrust their data.

53% integrate the privacy rights in a wider entity (40% in 2002). In that last category we find 28% that put the privacy rights in the general conditions or conditions to visit the website (56% in 2002). 11% insert this information in the customer's service, a webpage, sometimes as a FAQ-page where customers can find information about their rights (5% in 2002). 45% mention those rights only on the electronic form (26 % in 2002). 16% thought about alternatives, such as a disclaimer (13% in 2002). In a few cases the privacy statement appears once the personal data have been entered and sent. This is clearly too late. Before the consumers release their personal data, they have to be made aware of their rights and of the privacy policy of the organisation in general. The follow-up of the 2001 analysis indicates that an increasing number of websites are giving a place of honour to their privacy pledge. But when we have a look at the websites that mention their privacy policy in a specific section of their website, we observe that less websites integrate this information in an electronic form. Moreover an increasing number of sites enumerate the privacy rights in the general conditions, which can augment the risk that consumers do not browse through this list of conditions and other information concerning the use of the website, before filling in an electronic form. In other words, the privacy pledge can drown in an overflow of information.

When the privacy statement is put on a separate webpage, how is this webpage accessible by the visitor? In 30% of the cases the privacy page is accessible through the homepage (26% in 2002). So, from the beginning of the visit of the website the consumer can inform him- or herself about the privacy policy. 23% of the websites with a separate privacy page make this accessible by a hyperlink (eventually a symbol) that stays in the table of contents of the website (13% in 2002). This way a visitor, even the homepage left, can easily return to that privacy policy. 21% of the sites link the electronic form, where data can be brought in, with the separate privacy statement (12% in 2002). Finally the link between the website and the privacy page occurs otherwise on 26% of the sites, namely through a word or logo underneath each webpage (27% in 2002). Sometimes, this word and hyperlink ("policy", "disclaimer", "conditions", "site policy") is reproduced in very small font or sometimes a colour that is difficult to remark on the background (f.e. light grey on a white background). In addition, the visitor has to scroll all the way down the webpage to find the link to that information. Sometimes a visitor has to click through several levels of the site before finding information about the privacy policy. It is also remarkable that some multinationals with a website in the .be-domain, have a link with a privacy statement in English, that complies with some *Fair Information Practices* (principles of self-regulation concerning the use of personal data, cfr. infra), but not with European or Belgian legislation. Also the use of English terms such as "legal disclaimer" is not really consumers friendly in a website aimed at Belgian consumers. Words as "privacy" or "your rights", in English and, if needed translated in one or several of the national languages can be more informative. A privacy statement should be, strictly speaking, easy to find on a website. But above all, this information must absolutely be accessible on a webpage where an electronic form is inserted (eventually through a hyperlink

or a pop-up window). Before a website visitor releases information, the internaut must have the possibility to read the privacy statement.

3.3. Is the privacy statement complete?

A step further is the analysis of the contents of a privacy statement and the answer to the questions: does it correspond to the legal obligations? Do some firms go further than their legal obligations? How do the privacy statements score concerning clarity and completeness? The answers allow us to judge the quality of the privacy statements.

Before all, the responsible person for the dataprocessing must be named. In short, website visitors, who will release their personal data, have to know to whom those data will be entrusted. 45% of the websites gathering data identify the responsible person for the processing (74% in 2002). But, how detailed is that information in the privacy statement: 90% mention the name of the organisation, 23% have even a specific responsible department, 4% only name a person who can be contacted without giving more information about his or her function. No privacy statement mentions clearly a “privacy officer” or “dataprotection officer”, an employee answering the specific questions about the privacy policy (and other consumer's right) and responsible for checking and updating the privacy policy of the company.

The privacy law defines that a responsible for processing has to mention also his address. 65% do it. 10% mention a telephone number in the privacy statement. 19% an e-mail address, which should make it easy to the visitor to contact the responsible with possible questions. 8% communicate several contact data.

Besides the identification of the responsible the consumer who gives data has to be informed about the goals of the processing. 85% of the websites having a privacy statement, mention the goals of the processing (88% in 2002). So, 15% of the privacy statements in 2001 and 12% in 2002 do not contain that essential information. But we have to stress that we cannot give an opinion over the completeness and the quality of this information. Namely we can't verify in this analysis of websites if the communicated goals correspond with the real purposes of the processing within the organisation.

We will though in our e-mail response test, by sending an e-mail to the organisation, receive some surprising information concerning the real goals of the data processing (cfr. infra).

It is conspicuous that among all websites analysed in this research, collecting personal data online (as well the sites with a privacy statement as the ones without), 37% in 2001 and 49 % in 2002 communicate wherefore these data will be used. So a majority of the websites collects personal data without mentioning that fundamental information.

Which goals have been communicated on the websites, is a next question we want to answer. 34% of the privacy statements communicate that the data are necessary to process and fulfill an order (30% in 2002). 8% talk about a subscription that the consumer wants (13% in 2002). 60% state that the data will be used to keep the consumer informed about their products and services. In other words, 60% of the privacy statements announce that the data will be used for direct marketing (79% in 2002). 15% mention that the data can be used by another organisations for direct marketing purposes (also 15% in 2002). 59% of the privacy statements communicate also other goals, mostly vaguely formulated and not really informative for the website visitor, such as “internal use”, “commercial and contractual actions”, “administration of the website”, “making the website more user friendly”, “offering an as good as possible web experience” (20% in 2002). In these last situations, namely to update the website by adapting it to the characteristics of the visitors, there are often no personal data necessary. One can be interested in the age, language, gender and other

characteristics of the visitors, but these characteristics must not necessarily be linked to individual personal identification data (such as name, address, ...). Sometimes the hazy goal “internal use” is coupled to “contractually associated organisations”, by which the visitor knows no better about the final goals of the processing of his or her personal data.

When we compare some results from 2002 with 2001, we can conclude that there is a slight increase of the information concerning the purpose of the data processing. A larger significant increase is observed concerning the information about the data collection for direct marketing purposes.

As a large majority of analysed websites collects data and only a part thereof (43% in 2001 and 55% in 2002) has a privacy statement, we ask ourselves if in that statement the essential privacy rights of the concerned persons are mentioned. Moreover, are easy to use procedures proposed to exercise those rights? We will now have a look at the three fundamental rights, namely right to access your own personal data, to correct mistakes and to oppose to the use of personal data for direct marketing.

3.3.1. Right of access to personal data

In 68% of the privacy statements it is mentioned that the persons concerned have a right of access, namely that the consumers can have a look at their own data by contacting the responsible or by another user friendly procedure (73% in 2002). A third of the websites having already a privacy statement, do not mention that right, although granted in the privacy law of 1992. Of all the surveyed websites (with or without a privacy policy) that collect personal data, one third accords the right to access your own data.

But how can the consumer exercise that right concretely? Only 25% mention a postal address where the consumer can exercise his or her right (37% in 2002). 4% enclose an e-mail address (11% in 2002). 15% allow the persons concerned the possibility to look online, with a login name and password, into his or her own data (16% in 2002). 54% of the privacy policies do not mention any procedure to verify one's own private data (43% in 2002). The internet though offers an easy to use procedure to check and possibly correct personal data online, yet a lot of websites do not give the possibility to do this online in a secured environment.

By comparing both researches concerning the right of access, we can conclude that more privacy statements are informing the internauts concerning this right and less websites lack information concerning procedures to exercise that right. The most consumerfriendly and easiest possibility to access (and if necessary correct) personal data, namely using a secured online form is not yet the procedure that is adopted by most businesses that offer a right of access.

3.3.2. Right to correct mistakes in personal data

71% of the privacy policies mention the possibility to correct one's own data if faults have been found (78% in 2002). Of all sites collecting data, 32% point out the possibility to correct one's own data (that corresponds more or less with the percentage of websites that mentions the right of access).

How can a consumer correct his or her own data? Does this happen by sending a letter to the responsible or can he or she correct data online? 26% give the opportunity to the consumer to exercise this right of correction by post (37% in 2002). 4% mentions a specific e-mail address for this purpose (13% in 2002). Do not forget that there can be an e-mail address somewhere else in the privacy statement (or in the website) where the consumer can express that or other requests.

In 16% of the cases the consumer needs neither pen nor paper, nor has she or he to send an e-mail. The consumers can instantly online via a login name and password correct, if necessary, their own data (18% in 2002). 50% give no information about the procedure to follow for correcting faulty data (51% in 2002). We can conclude that in 2002 there is a slight increase of the information concerning the right to correct personal data. Again the online procedure to do so, is not yet adopted by a majority of websites.

3.3.3. Right to oppose to the dataprocessing for direct marketing purposes

Among those who mention explicitly in their privacy statement that the data will be used for direct marketing, 73% communicate that the persons concerned has a right of opposition against that use of their data (89% in 2002). Although that, at the moment of the first analysis of our sample, this right of opposition was not yet in force in the domain of direct marketing, it has been applied by a large majority. Moreover, there has been a significant increase in 2002. In other words, almost nine out of ten websites collecting personal data and mentioning in their privacy policy that these data will be used for direct marketing, communicate that right of opposition. We herewith repeat that in 2002 79% of the surveyed websites collecting data declare that these data will be used for direct marketing (60% in 2001).

How does the consumer have the opportunity to oppose against the use of personal data for direct marketing? 30% granting a right of opposition, inform that the consumer has to contact the business by traditional post if she or he does not want to receive any direct advertising (43% in 2002).

13% in 2001 and 12% in 2002 grant the person concerned the possibility to check a box giving explicitly the permission that her or his data may be used for direct marketing (opting-in). Although the opting-in regime is not yet installed in Belgium, some companies have already adopted this kind of permission marketing.

It happens sometimes that the opt-in tick-box is already checked, in other words it is suggested that the consumer wishes to be on the mailinglist, for instance, of the company. This is, in our view, not a consumer friendly opting-in giving a free option. In fact it is an opt-out, because one has to 'uncheck' the box to make clear that he or she does not want e-mailings.

30% in 2001 and 24% in 2002 choose the opting-out procedure, the consumers may check a box if they are opposed to the use of their data for direct marketing purposes. 26% do not give any details about how to exercise that right (21% in 2002). In a follow-up survey we will observe how the new Belgian law concerning a.o. the opting-in system will change this aspect.

Only one website refers to existing Robinsonlists (also called Preference Services) for direct marketing. These Robinsonlists are nationally and internationally managed databases wherein consumers refusing to receive direct mail (then we talk about Mail Preference Service), telemarketing calls (also named Telephone Preference Service) or (in some countries) e-mailings (the e-Mail Preference Service or e-Robinson, such as <http://www.e-mps.org>) can insert their co-ordinates. Concretely, the consumer will receive no commercial e-mails of firms that are member of one of the umbrella organisations of direct marketing, managing this e-Mail Preference Service.

If data are passed on to thirds for direct marketing purposes, then in half of the cases the right of opposition is offered (52%). We stress that only 15% (in 2001 and 2002) of the surveyed websites (collecting data) communicate expressly to pass the data to thirds. So, it consists of a small number of the visited websites. For this reason these results are given very cautiously. This right of opposition can be exercised in 33% of the cases by contacting the business by post (35% in 2002). 9% grant an opting-in (13% in 2002), 38% an opting-out through a tick

box (42% in 2002). 19% does not mention any procedure (10% in 2002). Also this aspect will normally be affected by the new Belgian law and will be studied in a next survey.

3.4. Additional information

In 38% of the studied websites an order can be made online. Sometimes orders can be made not only in the webshops but also in certain corporate websites of companies with a shopping corner. When we are in front of an electronic form, then we receive in 33% of the cases a clear signal on or near that form that we will enter our personal data in a secured environment. In 29% of the order forms additional information is given about the protection of the transaction. Some website managers are even so confident that they "accept credit card data through a secure server. 100% safe". A majority of websites divulges nothing about the security of the online registered personal data.

Besides the identification of the responsible (person), the goals of the processing and the privacy rights of the consumer is there any other interesting information given in the statement? For example, a concrete reference to the law exists in 47% of the privacy statements (56% in 2002). A majority refers to the law as "the law of 8 December 1992", but for the consumer this is far from informative. Very seldom one refers to the new legislation (of 11 December 1998). Only a few times one names the "law on the protection of privacy" or "privacy law" and other alternatives. We can try to explain this increase of reference to the law by stressing that after the new Belgian law came into effect, some media coverage could have inspired more marketers and webmasters to know the law and refer to it in their privacy pledge.

The only absent instance in the majority of the privacy policies is the Privacy Commission, the watch-dog of the privacy law that a.o. gives advice to the government and parliament, supports the citizen in the application of his or her rights and where more information can be obtained concerning the law. In a few cases the co-ordinates of that Commission are mentioned (12%). It could be interesting to have a hyperlink from the name to the homepage of the Commission (cfr. <http://www.privacy.fgov.be>).

On some websites minimalist 'privacy formulas' are shown, such as: "We respect the privacy law", "The privacy of the visitor is protected", "Your privacy is 100% guaranteed", or "We respect the law of 08.12.92", that supposes that the consumer puts automatically the link between the date and the privacy law. Other privacy statements exaggerate the other way, namely too formal, too tedious, too much details. They are more boring than interesting and inspiring confidence (for examples, cfr. Walrave, 2001a & 2001b). Certain statements are submerged on a webpage about general conditions. They do not present the protection of the privacy as the in-house philosophy and do not attribute a place of honour to it. In the mind of those website managers it is only a legally obliged formula that has to be mentioned somewhere on the website. Such, often hardly intelligible, formulas give a very consumer-unfriendly impression. Now and then the consumer's rights are disregarded bluntly and the privacy statement is only written from the firm's and not from the consumer's point of view. It becomes then a kind of 'disclaimer', trying to get rid of as much as possible responsibility. This 'privacy statement' is sometimes reduced to an 'enter at one's own risk'-warning.

It is advised to put a concise but a complete and easy to understand privacy statement on or near an electronic form where the visitor will enter personal data. More details, answers on specific questions could be put on a FAQ-page (Frequently Asked Questions). Privacy can be a chapter on the general FAQ-page, or a separate webpage can be dedicated to as well the privacy policy as to the technological protection of the data, the transaction and other consumer's rights. If the website is drawn up in different languages, it is recommended that

the privacy statement is formulated in those different languages. The style and vocabulary used must be adapted at the target group(s).

3.5. Are cookies been used?

As announced in the introduction to this research, we have analysed one way of implicit datacollection. In our first analysis 51% of the websites used cookies. This has increased to 67% in 2002. The sender of a cookie is in 76% of the cases the server of the visited website itself (73% in 2002). 16% of the cookies are sent by one or more thirds, such as online marketing businesses (12% in 2002). In 7% of the cases the cookies are sent by the website as by outside companies (11% in 2002).

Are they session-cookies that disappear after the visit to a website or are they permanent cookies that can be repeatedly recalled and altered at each session? One third of the cookies (34%) are session-cookies. They are only active during the visit of a website and disappear when the visit is finished. A status quo of 66% of the cookies can be recalled at future visits (even very often until a remote date somewhere in 2030).

If a visitor sets his browser up in a way that cookies are not automatically accepted, but that a warning pops up first, will the visitor receive access to the website if the cookies are rejected? In 33% of the cases where cookies have been rejected, access to the site is granted without any problems (22% in 2002). In 55% of the websites the cookies appear repeatedly, and disturb the surfing (68% in 2002). Although access to the site is granted, the cookies, that the user can accept or reject, reappear again and again. In 11% of the cases no access to the site is granted if cookies are not accepted on the homepage (10% in 2002). Sometimes a webpage appears suggesting to accept the cookies.

Exceptionally reasons are given why cookies are necessary to visit the website. In 12% (status quo in 2002) of the cases the visitor is informed about the use of cookies in the privacy statement or in a separate page where legal aspects or general conditions are explained. Among them 6% only mention in the privacy statement what a cookie is. 34% go further and explains what will be the use of those cookies. 28% give information about cookies, their purpose and how to switch them off. 31% give yet complementary information. But 88% of the websites using cookies do not give any information about the goal and use of cookies.

3.6. The e-mail response test

The e-mail address in some privacy statements incited us to verify to what degree a company can answer a simple question about the privacy policy. We have sent a question by e-mail⁵ not only where a privacy policy was present. On each website asking for personal data we have addressed a simple request concerning the goals whereto these data will be used.

On a request 57% did not answer in our mystery e-mail campaign in 2001 and 51% in 2002 (even by sites guarantying a response within 24 hours). The sites, that answered, needed a few minutes or replied up to ten days later. Among them who answered, 78% replied within 24 hours.

What was the quality of the answer, has the question been answered specifically and personally? 65% replied to the question in a specific, informative and personal way (63% in 2002). 15% give a standardised answer, sometimes via an auto-responder (21% in 2002). 17% thanks the consumer for the request, but does not give an answer to the question (11% in 2002). In a few cases we received an 'out of office'-response, where the employee responsible for answering the e-mails, is absent and the e-mails are not sent through to a present employee.

Some e-mail answers are very informative about the final goal of the dataprocessing. For example, in a certain privacy statement there is mentioned that the data will be used for "internal use" only. But asking more explanations by e-mail, we find out that they mean "own direct marketing actions". One poetic webmaster replies that the data are for direct marketing because "using the site is free of charge and we can not live on the dew only".

In a few e-mails one steps quickly over the question but one proposes directly to remove the data out of the database. But the question of the visitor was limited to information about the goals of the processing. Certain businesses associate the question about privacy instantly and solely with technological dataprotection. They reply then also that the data are secured adequately, but do not give any information concerning the goals of the dataprocessing (e.g. "Be reassured. Your data are secure in our hands!"). Although the secure storing of personal data is absolutely necessary, we have to stress that the protection of the privacy online is more than this: namely, the management and use (in conformity to the legislation) of personal data as agreed explicitly with the consumers.

Some answers of businesses give food for thought, as they answer that the data are 'momentarily' not used for direct marketing. Some add to this that they cannot foresee what will be done with those personal data in the future. Herewith it should be desirable to inform the persons concerned if the privacy policy changes and if the data will be used for direct marketing, for example. And in that e-mail the consumer should have the possibility to mention his or her choice. If the goals, for which the data have been collected, change, then this does not correspond any more with the conditions accepted by the consumers at the moment they released personal data. The persons concerned must be consulted again and have the choice, if they wish to reject these new usage conditions.

The contrast in the results of this e-mail response test is great between the companies that answer fast, politely and completely and the others that do not answer at all or sometimes reply with a short and blunt e-mail. For example, in the style of "all information can be found on the orderform", which finally is untrue as nothing is written about the privacy rights.

We have experienced that more than half of the websites does not answer a simple request about the processing of personal data. This can point out several malfunctions within the organisation. Firstly, we must not forget that a major part of our sample of websites have no privacy statement. The information about that subject has maybe never be communicated internally to the persons who have to answer the e-mails. We state also that with the increase of quality and completeness of the privacy statement, the quality and speed of the answer increase also. In short, a privacy strategy must not only be an accessory to evoke confidence in the show-window. The privacy statement must be experienced within the organisation and not be just some window-dressing. This can only if the employees, dealing with the personal data and replying the e-mails, letters and telephone calls of the customers and prospects, are themselves informed about the legislation and the application of the law within their own company. Clear internal communication about the privacy policy must precede the external communication.

3.7. The final score

As conclusion of the analysis of the privacy statements we repeat the final score of all websites we have analysed. On the basis of the privacy law minimal information must be communicated about: the responsible, the goals, eventually also the right of access and correction. The new privacy law adds the right of opposition when data will be used for direct marketing.

On the basis of the pure legal aspects actually in force, the websites collecting personal data score as follows:

	2001	2002
Identification of responsible	21%	40%
Information about the goals	37%	49%
Information about right of access	33%	41%
Information about right of correction	33%	41%
Information about right of opposition	20%	31%

Table 3: Percentage of websites collecting personal data that respect the obligations of the privacy law.

Herewith we stress that those percentages are about all the surveyed websites collecting personal data online. We repeat that in the survey 93% in 2001 and 90,5% in 2002 collect data of visitors in one way or another. Thereof half, has a privacy statement where the legally obliged information can be inserted.

A majority of the websites score highly unsatisfactorily for the information of the visitors about their privacy rights and about the procedures how to apply, if required, these rights. We want to stress though that the quality of the privacy statements is improving.

Besides, this minimal information obliged by the legislation, we have verified to what degree the sites communicate eventually also other information. 21% of all sites processing data mention explicitly the privacy law, whereas 12% mention the Privacy Commission. 5% have also a privacy label (mostly on the homepage) or refer to an ethical code whereon their privacy strategy is based (cfr. Walrave, 2001b).

4. How does Belgium score with respect to other countries?

If we compare these results with foreign research, namely in France and in the United States, then we come to the following conclusion.

In France the responsible for data processing is submitted to a certain number of obligations (Loi N° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, cfr. <http://www.cnil.fr/textes/index.htm>). Actually this law is to be adapted to the European dataprotection directive.

Stimulated by the twentieth anniversary of this law, the CNIL (the French Privacy Committee) took the initiative to visit hundred websites and verify if they were conform to the legal obligations. The CNIL restricted itself to e-commerce sites where visitors could buy products.

There has been stated that 69% of these contain information about the privacy policy. In our survey in Belgium 43% gives this information in 2001 (55% in 2002). But we had noted that for the e-shops that percentage was higher, namely 54% in 2001 and 61% in 2002. This is still lower than in France.

81% of the French e-commerce sites using cookies, do not give any information about the cookies, in Belgium 88%. But 20% of the Belgian e-shops using cookies give information about them.

52% (France) do not explain how to exercise the right of access, 54% of the Belgian websites (in 2001), but 60% of the Belgian e-shops.

We observe also in this short comparison of some results from the French survey with the first Belgian analysis of websites, that France's scores are higher concerning the integration of a privacy statement on the website. But for other questions the Belgian as the French e-commerce sites score on the same level. We repeat that the French law exists from 1978 on, compared to the more recent Belgian law of 1992.

In the USA, the Federal Trade Commission has surveyed to what degree privacy statements are present on the websites and what that privacy policy really covers (cfr. <http://www.ftc.gov>). From an analysis of a random sample of American websites, 88% have a privacy statement. The contents of these statements although is difficult to compare with the information to be given to website visitors, whereof data is collected in the European Union. When the surveyors verify the quality of these privacy statements, then the results are less optimistic. 20% of the privacy statements contain all four principles of the *Fair Information Practices*, these are the rules of conduct recommended by some international organisations (OECD among others), associations of businesses and (American) privacy organisations, namely:

1. Notice: information about which data they collect, how (as well explicitly as implicitly) and for which goals the data are necessary and if data are passed to third parties. A website has also to inform its visitors about the three following principles.
2. Choice: The consumers whose data are collected must have the choice how their data will be used besides the use wherefore the data initially were collected. It concerns an internal secondary use, such as own direct marketing campaigns, and external secondary use, such as hiring out of data to third parties for direct marketing.
3. Access: Consumers must have access to their data and have the opportunity to correct possible faults.
4. Security: The website manager must develop procedures necessary to secure the personal data.

41% of the analysed websites contain "notice" and "choice". On 8% of the websites a privacy label is displayed (in Belgium 5%). Thus, those initiatives of self-regulation are very seldom applied. When data are used for direct marketing, than we observe that 50% offer a choice. 25% propose an opting-in. 71% an opting-out. 18% of the sites accord the right of access and correction. The FTC concludes that although progress has been made, the initiatives of self-regulation are insufficiently followed up. The survey shows, according the authors, that self-regulation is not enough for the guarantee of a general implementation of a number of fundamental privacy principles. The Commission stresses the important role of self-regulation, but advises that the American Congress takes legislative initiatives in order to ensure, together with professional codes of conduct, an adequate level of online privacy protection (cfr. FTC, 2000).

Finally, an international comparative research of Consumers International was done by 13 national consumers organisations (cfr. <http://www.consumersinternational.org>). 751 websites in the USA and the EU (whereof 9 Belgian sites) were surveyed. The survey makes a difference between the general random test, the most popular websites and a few categories (retail, financial websites, health sites). In this summary we restrict ourselves to the results of the random test.

67% of the visited websites collect data of the visitor. Name, e-mail and postal address are mainly asked. In order to consult 7% of the websites one has to release personal data before that site can be entered. One third of the sites tries to place a cookie on the visiting computer. 58% of all visited sites collecting personal data have a privacy statement. Only 32.5% offer the possibility to consult the privacy statement on the page where data are collected (on the electronic form). In 63% of the cases the privacy statement was easily accessible from the homepage. If the privacy policy is not found on the website, then the surveyor had to e-mail the organisation involved to ask more information about the policy. Only 17% of 177 e-mails

have been replied to. This shows, according to the researchers, a lack of interest and involvement by many companies for privacy.

Concerning the use of data for direct marketing, the researchers observe that only 20% of the sites give expressly the choice if the consumer wants to be inserted on the own mailinglist. 9.5% give that choice when it concerns direct marketing for third parties.

About the contents of the privacy statement, the purpose of the database is the mostly communicated item (52%). Why data are collected is an item in 48% of the privacy policies. 42.5% communicate with whom the data will be shared and for which goals. 17.5% offer certain choices about the own personal data.

14% inform the consumer how he or she can be deleted from the mailinglist of the company. 18% give the possibility of access to own data and 31% to correct them. Moreover, 16% grant the possibility to remove the own data from the database. 22% of the privacy statements inform the consumer about the technological protection of the data. Finally, 6% mention the period of the conservation of those personal data.

The surveyors conclude also that nevertheless the legislative initiatives by European and national authorities, the consumer's privacy is not adequately protected on the internet. As well in Europe as in the USA the websites fail to apply the fundamental international directives concerning the protection of the privacy.

5. Conclusion: still a good deal of work to do

The integration of feedback possibilities for individual consumers to advertising messages becomes a priority of marketers. The use of direct and interactive media, moreover, offers the possibility to scan the behaviour of prospects and clients. Knowledge about consumers is built, not only about their buying intentions or perceptions of and attitudes towards a company or product. Actual behaviour of individual consumers is stored in databases and analysed to inspire personalized communication.

Marketing on the internet is, at the moment, the pinnacle of this trend. Banners and intermercials cannot only be broadcasted on a website, where the visitors more or less have a similar profile as the target group of the advertiser. Advertising on the internet can namely be sent to the browser of an individual visitor of a website, depending on his or her profile, the webpages visited, the search commands entered, the electronic form filled in. Besides, more individualized and detailed information can be sent by e-mail.

The communication process between the consumer and the website can be a learning process, in which the offers and services of the advertiser can be adapted real-time to the questions, hints, surfing behaviour of the prospect.

In this first survey of Belgian commercial websites concerning the protection of privacy and concerning the application of the Belgian privacy law, we observe that a majority of the visited websites does not give any information to the website visitors releasing their personal data online. It is notable that many businesses try to make the navigation in their website user-friendly and to enlarge the possibilities of interaction and feedback. This way they want to fulfill the wishes and necessities of the website visitors. But for the management of the personal data, the consumer loses all control in many cases.

How can it be explained that, more than seven years after the original Belgian privacy legislation and in the year wherein the new (more stringent) law is put in force, the privacy policy of many websites is deficient or non-existent?

Firstly, we suspect a lack of knowledge about the consumer's rights, that have to be respected on the internet, but also in distance selling in general. Maybe a great uncertainty exists about which legislation is in force in internationally directed websites. Besides we can attest that the obligations, that a website has to meet, are dispersed over several laws. Some European

directives are already converted into the Belgian law, others not yet. In short, for the beginning manager on the internet, it is sometimes a real puzzle to gain discernment in the rights of his website or e-shop visitors.

That e-shops score better than general corporate websites, can maybe be explained by the fact that an online shop wants to offer all possible guarantees in order to incite the visitor to buy. The e-shops are also subject to the regulations for distance selling. Postorder companies, teleshopping channels and other shops going online, have already the necessary experience in that domain. As e-shops collect also sensitive data (credit card number, ...) guarantees about confidentiality of these data is a must.

Besides, we suspect also a lack of knowledge of the website managers about the sensibilities, (preconceived) opinions and priorities of internet users. Considering that the effectiveness of online advertising and direct marketing can be measured better and better and also the number of visitors on a site and their surfing behaviour, one looks maybe only at the quantitative measurements to evaluate one's online communication. Internet marketing, and online and off line direct marketing are very response pointed. The results of the communication are mostly evaluated only by quantitative standards over a short period. How to stimulate the trust, the long-term loyalty receive less attention, as these hardly measurable aspects contrast violently with the huge volumes of data generated by the surfing conduct and the transactions.

But we are convinced that, in order to gain the consumer's confidence, the website visitor must be better informed about her or his rights and among other things about the privacy policy of the online business. In the online and off line direct marketing there is always an ear for the wishes and the needs of the consumer about products and services. But what is the consumer's appraisal of and critics about the direct and interactive communication, that the firm uses to try to create a relationship with him or her individually? How strong or weak is the confidence of the consumer in the handling of personal data? These questions are still very often neglected by many businesses.

The European dataprotection directive and the national privacy laws create maybe the opportunity of reflection about these questions. The corner-stone of the (Belgian) privacy law, and also of the European data protection directive, is the transparency by which the personal data have to be collected and processed. In our research we observed too many times that the contact with individual website visitors is used as a unique occasion to gather as much as possible personal data.

A (small) incentive is used to stimulate the consumer to fill in a questionnaire. In the majority of the cases no information is given about the purposes and the utility of this collection of personal information. Although the individualisation of a website's contents and of the offer of products and services is vital for the future of e-commerce, clear engagements have to be made between the responsible (person) for the data processing and the consumers involved, about the management and the use of personal data.

The privacy law could generate a mentality switch: namely, each person, or decision maker of an organisation, who processes data, must, before starting the collection of the data, meditate about the purpose, the necessity of the data, the privacy rights of the persons concerned and how they can exercise these rights. The clear and simple formulation of this information in a privacy statement on a website, is not only a legal must (besides other legal obligations), but contributes also, in our opinion, to as well the trust in the company that runs the website, as the confidence in e-commerce in general. A company cannot therefore build one-to-one, long-term and loyal relationships by analysing only the wishes, needs and complaints of consumers concerning their products and services. Marketers have also to be all ears for the wishes and remarks of consumers concerning the use of their personal data and the media used to communicate with them individually.

Bibliography

- Allen, C. (1999), *Internet World Guide to One-to-One Web Marketing*. New York: Wiley Computer Publishing.
- Bazsalisca, M.; Naïm, P. (2001), *Data mining pour le Web. Solutions d'Entreprise*. Paris: Editions Eyrolles.
- CNIL (1999) *Protection des données personnelles et e-commerce en France*.
- Consumers International (2001), *Privacy@net. An international comparative study of consumer privacy on the internet* (<http://www.consumersinternational.org>).
- Dinant, J.M. (1999), *Les Traitements invisibles sur internet*. Namur : CRID, FUNDP, (<http://www.droit.fundp.ac.be/crid>).
- FTC (2000), *Privacy online: Fair information practices in the electronic marketplace. A report to congress*. (<http://www.ftc.gov>).
- Gelman, R. (1998), *Protecting Yourself Online*, San Francisco: Harper Edge.
- Peterson, C. (1999), *I love the Internet, but I want my privacy too!* Prima Publishing.
- Thomas, P. e.a. (2001), *Avis N° 34 du 22 Novembre 2000 Avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique* (<http://www.privacy.fgov.be>).
- Walrave M. (1999), *Privacy gescand?*, Leuven: Universitaire Pers.
- Walrave M. (2001a), *e-Marketing and Privacy. Privacy Paper Nr. 1.*, Department Communication Science, Leuven: K.U.Leuven.
- Walrave M. (2001b), *e-Marketing & Privacy*, Diegem: Kluwer.
- Walrave M. (2002), *e-Marketing et Vie Privée*. Diegem : Kluwer.
- Westin A. (1991), *How the American Public views consumer privacy issues in the early 90's and why. Testimony before the subcommittee on Government Information, Justice and Agriculture. Committee on Government Operations, US Government Printing Office, Washington D.C., April 10, 1991.*

¹ For more technical information see <http://www.cookiecentral.com>

² More information about P.E.T.'s cfr. Dinant: 1999, Walrave:2001b.

³ In the next e-Privacy Paper we will control the evolutions of the online privacy in Belgium and abroad. The results will also be tested to the priorities of the internet users.

⁴ For a more detailed comparison of the 2001 and 2002 analysis, an overview of good practices, positive and negative examples, we refer to the privacy paper Nr. 2 that will be published at the end of 2002.

⁵ We have not used our university e-mail address, but a more neutral one to avoid possible influence this official e-mail address could have on the answers.