



# CONTENT

- ABSTRACT** ..... 3
  
- 1. INTRODUCTION** ..... 4
  
- 2. PROTECTING MINORS' E-PRIVACY** ..... 7
  
- 3. METHODOLOGY** ..... 9
  
- 4. RESULTS** ..... 10
  - 4.1. Data processing** ..... 10
  
  - 4.2. Presence of a privacy statement** ..... 13
  
  - 4.3. Content and completeness** ..... 14
    - 4.3.1. Identification* ..... 14
    - 4.3.2. Purposes* ..... 14
    - 4.3.3. Right of access and correction* ..... 15
    - 4.3.4. Objection to direct marketing* ..... 16
    - 4.3.5. Target group adaptation* ..... 17
  
- 5. CONCLUSION** ..... 18
  
- REFERENCES** ..... 19

## ABSTRACT

Young people are increasingly using different applications of the internet. In this context, they are commercial targets for advertisers, especially on websites designed for this target group. During their visits to these websites, personal data are often collected in an explicit manner (e.g. using electronic forms), as well as in an implicit manner (e.g. using cookies, click stream analysis). To protect the *informational* privacy (i.e. data protection) and the *relational* privacy (i.e. in this domain the right not to be contacted by companies by amongst others e-mail for marketing purposes) legislative initiatives have been taken in the European Union (e.g. European data protection directive 95/46/EC). Institutions have made specific recommendations to protect children online (e.g. the Belgian Privacy Commission and the Belgian Internet Observatory). Websites aimed at minors often collect personal data during their visit to allow them (free) access to information and games. But also in the context of contests and online services (chat, e-cards etc.) personal data of the website visitors and sometimes thirds are asked.

In order to check whether legal obligations were observed and recommendations applied, websites of organisations established in Belgium and mainly targeting kids and teens have been analysed. The results show that, while a majority (8 out of 10) collects personal data, only a minority observes the privacy rights of the young website visitors. This results from an analysis of 294 websites published in the fourth privacy paper entitled *Cyberkids' e-Privacy* by Prof. dr. Michel Walrave of the University of Antwerp (Belgium).

Privacy statements summarizing information concerning the identity of the responsible for the data processing, the purpose(s) of it and the specific privacy rights, are present in only a minority of websites harvesting personal data (4 out of 10). Furthermore, the privacy statements are often incomplete or do not use a phrasing adjusted to the target group. Also few companies involve the parents when collecting personal data, by informing them or asking their permission.

Therefore new initiatives of (co-)regulations could be taken to make clear when, for which purpose(s), how and which personal data of minors can be processed. How minors are informed about this and how they can exercise their privacy rights are important for the development and awareness of the growing-up consumers. Moreover, some explanation is needed about the circumstances in which the advice or permission of a parent is indispensable.

The purpose of the Privacy Papers is to investigate specific topics in the area of privacy protection in the information society in general and the internet in particular. Since 1992 prof. dr. Michel Walrave, author of the papers, is conducting research on the implications of the information society, especially (online) data protection and direct marketing.

More information can be found on <http://www.e-privacy.be/cyberkids.html>

# 1. INTRODUCTION

Currently, minors increasingly use the different applications of the internet. More and more content and services are aimed at young users. Children and adolescents are more exposed to commercial propositions and other offers such as contests, games and chat sites that request personal data. Therefore, they are not only a target of online marketing communications using webvertising (banners and internet commercials, for example), but also of a more individualized and interactive communication by processing their personal data for direct marketing purposes, using e-mailmarketing and mobile marketing.

Moreover, the internet (and other applications of ICT) changed the nature of the individuals' privacy, because companies are able to collect personal data using forms (i.e. *explicit* data processing), in which individuals entrust information explicitly to companies. Furthermore, specific software allows companies to monitor the individual's behaviour, based on the *click stream*, namely the surfing patterns of website visitors (i.e. *implicit* data processing). This often surreptitious data processing can be linked with personal data gathered in online forms but also off line collected information based on, among others, consumers' purchases. Companies are therefore able to draw a detailed profile of individuals to inspire targeted direct marketing communication. These practices create an area of tension between (online) marketing and personal privacy (Bazsalisca & Naim: 2001, Dinant: 1999, Milne & Culnan: 2002; Walrave: 2001; Walrave: 2004). This much debated subject has led to the distinction between informational and relational privacy (Schoeman: 1992, Westin: 1991).

Applied in online direct marketing, the *relational privacy* of an individual is the answer to the question whether or not, and possibly to what extent, a consumer wants to be approached by companies. Respecting the relational privacy means that a consumer is given the possibility to choose whether to be contacted for marketing purposes or not. This also forms a key aspect of the debate concerning *opt-in* (giving explicit permission to use data for direct marketing purposes) versus *opt-out* (the right to object to the use of personal data).

*Informational privacy* deals with the possibility of an individual to choose which companies are processing personal data and for what purposes. To be able to make that decision the purposes of the processing of personal data must be clear. This transparency is ensured if the data processing organization informs the individual entrusting personal data (i.e. the data subject) about how personal information will be used. This forms the cornerstone of the EU data protection directive (95/46/EC). Besides the privacy law, there are also other national laws and European directives regulating aspects of the protection of the informational and relational privacy<sup>1</sup>.

---

<sup>1</sup> A directive with important consequences for the online marketing industry implemented an opt-in regime for electronic commercial communication, using e-mail, but also text messages by mobile phone, for example (2002/58/EC). This directive came into effect in Belgium on 28 March 2003.

Based on this regulation, two Belgian institutions adopted recommendations concerning the protection of minors on the internet. The advice of the Belgian Internet Observatory, on the one hand, focuses on protection measures that can be used to prevent minors from being confronted with harmful content (Internet Observatory, 2003). The advice of the Privacy Commission, on the other hand, stresses the processing of personal data of minors. The latter official advice was adopted in 2002 and will be summarized below.

In the context of the research presented, we namely narrow down our scope to the application of the obligations of the data protection directive, transposed in the national privacy law for websites of companies established in Belgium whose main target are children and adolescents. We will also check to what extent companies are taking the suggestions of the Belgian data protection authority into account.

First of all, we enumerate the main obligations that need to be fulfilled when processing personal data. Three main principles underpin the data protection law. The *transparency principle* states that the data processing must include specific information concerning the identification of the person or organization responsible for the data processing (called *data keeper* or *data controller*), the objectives of the data processing and specific information concerning the privacy rights of the person involved (also called *data subject*). Secondly, only necessary data are to be gathered with respect to the aim or purposes of the data processing made known to the individual, i.e. the *proportionality principle*. The *fairness principle* states that the data controller needs to stick to his engagement with the data subject concerning the use of the data.

In the context of transparent online data processing with regard to the website visitor, the data keeper has to give the following information to the data subject who entrusts personal information (i.e. the transparency principle of the data processing):

- who is the data controller (in short, the natural or legal person determining the purposes and means of the processing of personal data) and where is this person or organization located (name and address);
- what is the purpose or are the different purposes of the data processing;
- how can one *object*, without charge and without giving a reason, against the processing of personal data for *direct marketing*;
- which data are indispensable (to fulfil an order, for example) and which information is optional. What are the consequences if all or some data are lacking;
- the possibility to exercise a *right of access* to own data and to *correct* mistakes;
- taking into account the specific circumstances of the data processing, additional information can be communicated, for instance: who are the recipients (or categories of receivers) of the data, if these data are not (only) used by the organization that collects them, but for instance sold or hired to others.

This is, in brief, the information that needs to be given to a person when processing his or her personal data. But, when and where must this information be given? The law indicates that the individual must be informed at the latest when the data are obtained. For example, a hyperlink on the homepage and/or electronic form(s) to a webpage with the privacy statement or legal information is a possible implementation of this obligation. The information can also be assembled in a privacy statement, displayed at the top of an online form. The privacy law also specifies that the right of opposition, in the case of direct marketing, has to be granted on the form where personal information is written down, using for example a simple sentence with a tick-box.

## 2. PROTECTING MINORS' E-PRIVACY

As already mentioned, two institutions have adopted a recommendation concerning the protection of minors online. The Internet Observatory stresses that no rules have been issued to protect minors on the internet, while such rules exist for other media such as television and cinema. Besides, the convergence between traditional mass media and telecommunications makes a legislative division between them less effective. Therefore, some general rules to protect minors in the information society should be drawn up. The implementation and enforcement of these rules can be based on a dialogue with specific sectors targeting minors. In addition, specialised control teams already organize national, European and international *internet sweep days* on which different specialized teams focus on the identification of law infringements (e.g. pyramid schemes and other scams). In Belgium, for example, the Internet Inspection Team of the Economic Inspection of the Federal Public Service Economy collaborates with the International Marketing Supervision Network on the sweep days, and information on cross border consumption problems is exchanged [<http://www.econsumer.gov>].

Hereafter, the advice of the Belgian data protection authority will be outlined. It was checked during the 'sweep days' organized in this survey concerning the implementation of data protection rules for websites mainly aimed at minors.

In its official recommendation concerning the protection of minors on the internet (16 September 2002), the Privacy Commission [<http://www.privacy.fgov.be>] has stressed that the implementation of data protection rules have to be more strict whenever minors are asked for their personal details. The Commission wanted to clarify the way in which the data protection rules apply to minors, taking into account the weaker position of this group and in some way also the fact that children are not able to take a critical attitude towards forms of marketing communication that can be hidden in entertainment, contests and other popular services. Minors, and often internet users in general, can be easily persuaded to entrust their personal details in these entertaining contexts.

The Commission emphasizes the need for a strict interpretation of the data protection principles in order to protect minors. In the official opinion of the Commission, there is a difference between children and youngsters. The transition is situated around the age of discernment (situated between 12 and 14 years). The Belgian legislation defines minors as individuals having not reached the age of 18. But starting from the age of 16 some rights are given to adolescents (Privacy Commission, 2002: 2). Therefore, also in the context of data processing the difference has to be made between age segments, and children deserve the most far-reaching protective measures. These include an active involvement of parents in the decision whether or not to entrust personal details. With this intention, the following statements are made concerning the interpretation of the main legal data protection principles:

- Regarding the *transparency principle*, the compulsory information concerning the privacy rights needs to be simple and accessible. Moreover, minors should be encouraged to discuss internet issues with their parent(s), especially when the processing of personal data is concerned.
- With regard to the *proportionality principle*, the Commission recommends that no identifiable information of minors should be collected (not only personal data such as name and address, but also pictures) (Privacy Commission, 2002: 4).
  - When asking an e-mail address, the individual should be recommended to give an electronic address that does not identify him/her personally but uses a pseudonym.
  - When offering the minor the possibility to subscribe to an electronic newsletter or to use a chatting service, only the e-mail address (using a pseudonym) can be asked. Other data such as name, address and other contact details are irrelevant.
- In respect with the *fairness principle*, the Commission states it is illegal to collect information of minors about their parents, family, friends (and for example their consumption preferences or other issues).
- Moreover, the processing of personal data for marketing purposes should not be directed towards children under the age of discernment.
- Finally, the Commission judges that the processing of sensitive data (such as medical information, data that directly or indirectly inform about the racial or ethnic origin, philosophy or religion or the sexual preference) cannot be collected from minors when they have not yet reached the age of discernment (Privacy Commission, 2002: 5).

As mentioned above, the Commission recommends the parental involvement or consent in some circumstances. This must not be an automatism for every data processing of minors. This would undermine the right of privacy of the minor. Nevertheless, it is important in some risky circumstances when minors do not oversee the consequences of the data processing and their enthusiasm could be abused. For that reason, the Commission judges the parental agreement necessary when the child has not reached the age of discernment, when sensitive data are collected from them, when the purpose of the data processing is not directly to the advantage of the minor (e.g. marketing and/or pass on data to third parties), or when data are destined to be published online (Privacy Commission, 2002: 6). Subsequently, the Privacy Commission addresses also questions concerning pictures of children (e.g. posted online by schools), and the identification of minors on websites not intended (and possibly harmful) for them (Privacy Commission, 2002: 6-9)<sup>2</sup>.

---

<sup>2</sup> Cf. also the first recommendation of the Internet Observatory [<http://www.internet-observatory.be>]

### 3. METHODOLOGY

Based on the obligations formulated in the law and the recommendations of the Privacy Commission, an online questionnaire was drawn up to analyse a sample of websites especially aimed at kids and teens. The purpose of this research consists of evaluating the manners in which personal data are collected on these websites and if this data processing happens in conformity with privacy legislation<sup>3</sup>.

The compiled sample was split into three main categories. A first group consisted of websites that mainly try to attract children (younger than twelve, 15% of the sample). This was decided based on cartoons, personalities, idols and other content and design characteristics of the website. The second segment of the website database gathers content targeting adolescents (45% of the sample). Thirdly a mixed category was compounded of websites that offer content and services to different young target groups (children and adolescents, 29%). Finally, some websites contained some pages for a young public, but also content and services aimed at adults (11%) (e.g. the webpages for young customers of a bank). In the analysis below, the two last segments form the miscellaneous category.

For the analysis of the websites, an online questionnaire was used to investigate not only how many and what kind of data were asked in online forms (i.e. explicit data processing), but also what types of cookies (i.e. implicit data processing) were sent (session cookies or persistent cookies, from the server of the website visited and possibly other servers)<sup>4</sup>. Next, we investigated whether or not, to what extent and how specific legal obligations were respected. Our analysis was concentrated on the access, form and content of privacy statements. We analysed how many websites were communicating the legally obliged information (i.e. quantitative analysis), how complete that information was and how it was communicated (i.e. qualitative analysis). The central question that we tried to answer in this research is indeed: is the young website visitor informed about the privacy policy by the data controller, and if so, to what extent is this information in conformity with the law?

---

<sup>3</sup> More information on the methodology to compile the sample of websites can be found in Walrave, 2005.

<sup>4</sup> The results concerning the use of cookies, but also the mystery e-mail sent to the website responsible, are discussed in Walrave, 2005.

## 4. RESULTS

### 4.1. Data processing

Concerning the explicit processing of personal data we have observed that 8 out of 10 (82.4%) of the analysed websites invite visitors in one way or another to entrust personal data: by means of an electronic form or a subscription to an electronic newsletter, an order form (7%) or a form asking for more information about products and services (46%). The possibility to e-mail to the webmaster (12%) is also considered as a processing of personal data, as the company obtains the e-mail address (and possibly co-ordinates and other information put in the message by the author). One third of the sites (34%) offer different options to pass on personal data. The data collected are summarized below in table 1.

<b>Identification</b>	
Name	81%
<b>Contact details</b>	
e-mail	87%
Address	54%
Telephone	32%
Mobile phone	19%
<b>Personal characteristics</b>	
Age/birth date	37%
Gender	15%
Nationality	6%
Household composition	2%
School	4%
Studies	5%
Hobbies	7%
Consumption	2%
Personal picture	3%
Other data	27%
<b>Information of third parties</b>	
Parents	0.5%
Friends	5%
Others	1%

Table 1: Types of processed data

One fourth of the websites (27%) also ask questions concerning the evaluation of the site or other questions related to the service (e.g. chat site) that they offer.

Websites that could be categorized as mainly targeting children, ask for personal details slightly less often (79%) than websites for adolescents (86%). In the miscellaneous category, 9 out of 10 websites collect personal information. This same proportion was registered in previous surveys (in 2001 and 2002) wherein a sample of 250 business-to-consumer sites was examined (Walrave, 2002).

If we compare these results with the advice formulated by the Privacy Commission we notice that still a majority (79%) of the sites ask for minors' personal data. The data asked in the websites for children are mainly the e-mail address (80%), the name (67%), postal address (44%), telephone number (telephone number: 22%; mobile phone number: 10%), age (36%) and on a few websites the name and contact details of third parties are also asked (6% of the sample of children's sites).

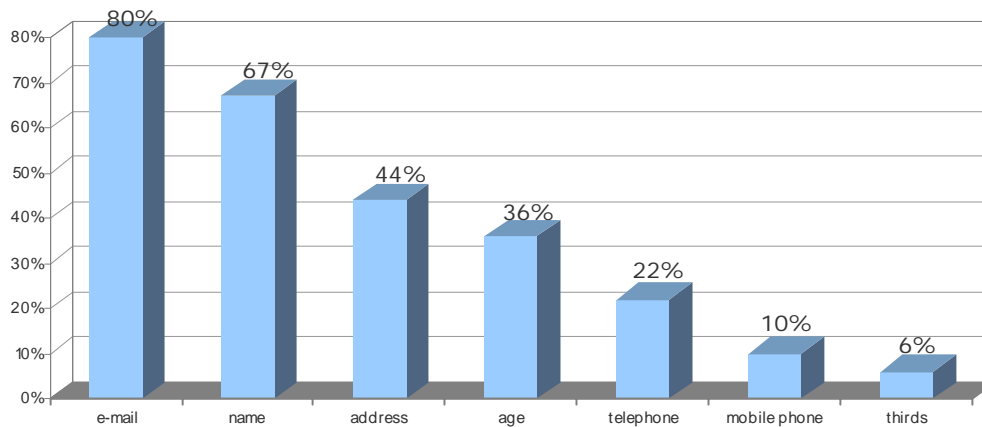


Figure 1: Processed data in websites mainly targeting kids.

The parents are rarely involved in the request of personal information of the children. Only a couple of webmasters ask the visitors to request the permission of their parents before filling in a form (3.5%). This is seldom combined with a concrete possibility for the parents to communicate their consent. One online form integrates an e-mail grabber where the child can insert the e-mail address of a parent. In another site children are asked to download a form that parents have to sign and fax before the registration is valid. Finally, some sites ask the young visitor to tick a box to confirm that parental agreement is obtained. Most attempts to involve the parents cannot be qualified as flexible and effective, although there is an attempt to encourage the young website visitors to discuss the data processing with their parents.

To have a view on the relevance of the data requested in the electronic forms, we investigated the context of the data processing. A majority of online forms are used to ask questions to the organization (31%) while one out of six (16%) asks personal details in the context of a game or competition. Other possible purposes are a membership to an organization (23%) and the registration for an electronic newsletter (24%). Furthermore, visitors can post comments to a guestbook (11%), participate in an e-survey (2%) or use the services that are offered (e.g. SMS-service, chatting, dating, 13%) or order products (18%).

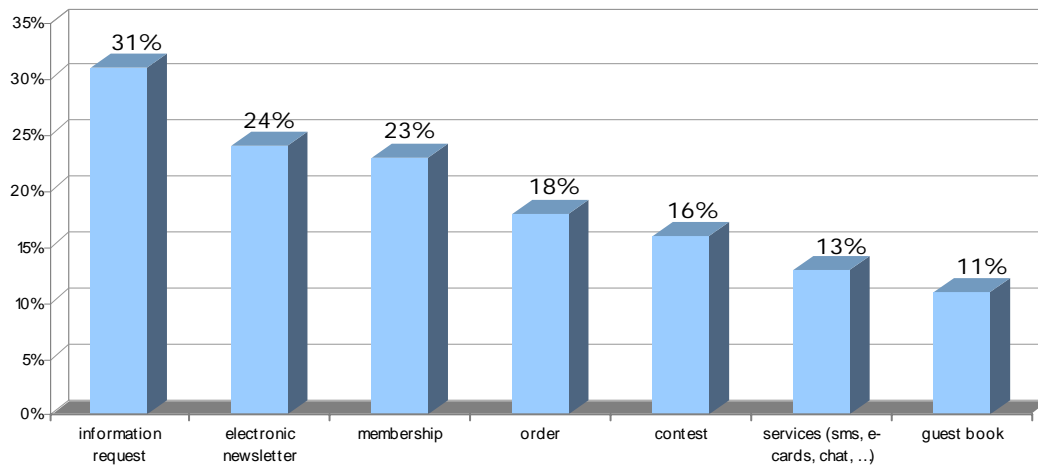


Figure 2: Contexts of data processing in kids and teens websites.

For a lot of services offered online, an excessive amount of data are asked for. An example: to obtain a free subscription to an e-zine, only the e-mail address is necessary. But, we noticed that several organizations link that subscription to a (sometimes compulsory) transfer of other personal data. This is not a peculiar characteristic of websites targeting young internet users. In a previous survey analysing general B-to-C sites the same tendency was noticed. This is why another characteristic of the online forms has been examined, namely whether or not a difference was made between necessary information and secondary data. Only a third of the sites (35%) offer the visitors the opportunity to choose which complementary data they want to entrust. We noticed that some websites collect data that are strictly irrelevant for the explicitly mentioned goal(s) of the data processing. These secondary data can be an interesting source of information about the website visitors and can also be used to remain in contact with them. Nevertheless, these additional goals must be explicitly mentioned. The consumers must have the choice to communicate extra information for additional purposes to control the use of their data.

## 4.2. Presence of a privacy statement

Only four out of ten sites (39%) processing data offer information in the form of a privacy statement. There is a difference between the websites for children (55%), adolescents (38%) and the other segment of the sample (33%). In the first category of sites half of the webmasters offer information concerning, amongst others, the purposes of the data collection and the privacy rights. Still, a majority of all sites surveyed do not provide any information that is legally compulsory.

Not only the content of the privacy statement, but also the form and the access were analysed. First of all, do companies give the privacy policy a place of honour on a separate webpage or is it part of an extensive policy or disclaimer with other consumer rights, copyright and other terms of use?

Half of the privacy statements (49%) are formulated on a separate page dedicated to privacy rights. The other half integrates the privacy rights in a larger text about legal aspects of the website or the general terms of use. Enumerating the privacy rights in the general conditions can augment the risk that website visitors do not browse through this list of conditions and other information concerning the use of the website, before filling in an electronic form. Furthermore, the privacy promise can drown in an overload of legal information.

The presence of a privacy statement does not automatically mean it is accessible for website visitors. Only one out of five (22%) websites including a privacy policy, link this information with one or several electronic forms. The presence of this link at the top of the electronic form (in two cases) offers a real opportunity for the individual to consult the privacy pledge before deciding to entrust personal data. Most websites offering a link to the privacy statement (fifteen cases) put the link at the bottom of the form. Some webmasters go a step further and offer an abstract at the top (three cases) or the bottom of the electronic form (eleven cases), which directly confronts the website visitors with their privacy rights.

In a fourth of the websites (28%) the privacy statement is accessible through the homepage. Less websites, namely one fourth (23%) put a link at the bottom of each webpage next to other information of the organization. In a few cases this hyperlink ("policy", "disclaimer", "conditions", "site policy") is reproduced in a small font or sometimes in a colour that is difficult to notice against the background (for example 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.

In this and previous research we have observed that some multinationals, established in Belgium and with a website with a ".be" domain name, have a link with a privacy statement in English. The use of English terms such as "legal disclaimer" is not really suitable for a website aimed at Belgian kids and teens. Words such as "privacy" or "your rights", in English and/or translated in one or several of the national languages can be more informative.

### **4.3. Content and completeness**

We now take it a step further. In the paragraphs below, we discuss the analysis of the content and style of a privacy notice and give an answer to the questions: does the privacy statement contain all compulsory information? How is this information formulated: in juridical jargon or in straightforward language adapted to the target groups?

#### **4.3.1. Identification**

First, the person responsible for the data processing must be identified. In short, website visitors have to know to whom they will give their personal details. Half of the statements (52%) identify the data controller. But, how detailed is that information in the privacy statement? Next to the name of the organization, some websites precise the department responsible or name a person who can be contacted. The privacy law clearly defines that a data controller also has to mention his address. This is the case in one third of the privacy policies (31%). A few sites mention other contact details - a telephone number (14%) and one fifth (20%) an e-mail address - which should make it easy for the visitor to contact the company.

#### **4.3.2. Purposes**

Besides the identification of the data controller, the consumer has to be informed about the purposes of the data processing. A majority of the statements (86%) mention one or several goals of the database. 15% of the privacy statements communicate that the data are necessary to process and fulfil an order. In one out of six (16%) the subscription to an (electronic) newsletter is mentioned. Half of the privacy statements (54%) declare to use the data to keep the consumer informed about their products and services. In other words, a majority of the privacy statements on websites mainly aimed at attracting kids and teens announce that the data will be used for direct marketing. Besides, 14% mentions that the data can be used by other organizations for direct marketing purposes. Let's remind that this is not a fair information practice according to the Privacy Commission when minors under the age of discernment are concerned.

Some privacy statements (13%) also communicate other goals, mostly vaguely formulated and not really informative for the website visitor, (e.g. "internal use", "administration of the website" or to adapt the website to its visitors). With these hazy phrases the visitors do not get a clear picture of the final goals of the processing of their personal data. One fifth (21%) also declares that the data are needed to participate in a contest, or a survey (12%), or to answer to a request of the visitor (19%).

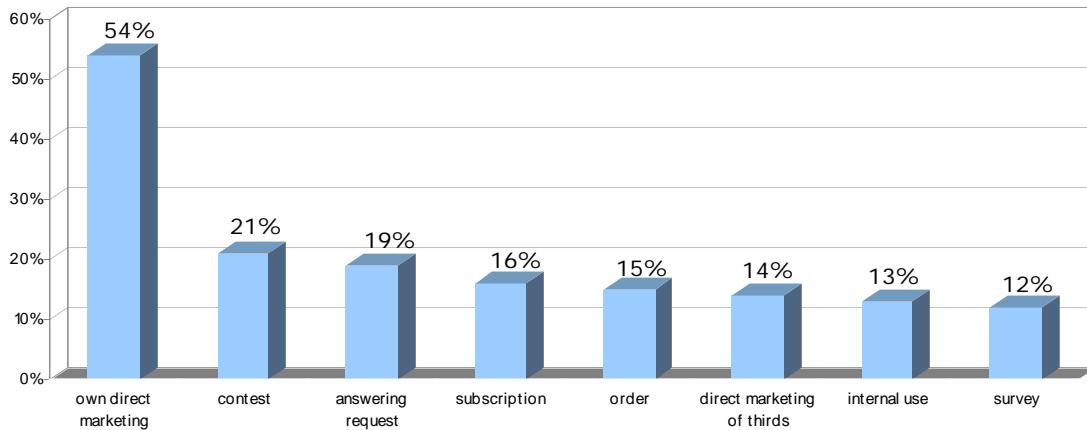


Figure 3: Purposes of the data processing mentioned in the privacy statement.

### 4.3.3. Right of access and correction

Besides identification of the responsible person and the purposes of the processing, one has the right to access personal information entrusted to an organization.

In a majority (67%) of the statements the right of access is mentioned. This also means that one third of the websites with a privacy statement do not mention that right, although it is already granted in the privacy law of 1992, that came into force in 1993.

But, how can the consumer exercise that right? In four out of ten statements (39%) no information is given concerning the procedure to follow to apply that right. The Belgian law does provide a procedure to follow when exercising this right. However, the legislator does not mention if or how to inform the individual about this procedure. So, the people confiding their personal data are not always informed how they can get access to their personal information. Of the sites that mention a procedure, 26 % declares that one can exercise that right by post. Some organizations declare in addition that they have created a specific form that can be asked for. About one third (30%) offers the possibility to request information by e-mail. A limited number of companies (13%) defining the right of access, offer a user-friendly and direct possibility, namely online access through a personal login and password. One fifth of the sites offer the internet user different procedures.

Although the internet offers an easy-to-use procedure to check and possibly correct personal data online and thereby to update the database of the company, a lot of websites do not offer the possibility to do this online in a secured environment.

A same proportion of privacy statements (66%) inform the visitor about his right to correct possible mistakes in personal information registered in the company database.

One fourth (23%) of the companies stipulating this right, give the consumer the opportunity to exercise this right of correction by post. A few more (26%) mention a specific e-mail address for this purpose. In 13% of the cases, the consumer can instantly access and correct data online. Four out of ten sites give no information whatsoever about the procedure to correct personal details.

Again, the most consumer-friendly and easiest possibility to access and, if necessary, to correct personal data using a secured online form is not yet the procedure that is adopted by most businesses.

#### **4.3.4. *Objection to direct marketing***

In more than half of the privacy statements the visitors can learn that the processed data are used for direct marketing. In that case the person responsible for the data processing has to offer a right to object. This is mentioned in 60% of the cases. Four out of ten sites communicating that they will use the data for marketing purposes do not present the possibility to object to this use.

When the data are collected directly from the individual, the legislator expounds that this right must be offered on the form itself. In contrast with the right of access and of correction, the procedure for the right to object is established. Only informing of the existence of that right is not enough. Consumers have to be given the opportunity to object if data are processed for direct marketing purposes. This can be done by incorporating a sentence with a checkbox that can be ticked if the visitor wants to oppose against the use of personal data for direct marketing (opt-out). A company can also explicitly ask the permission to use the personal data for sending commercial messages (opt-in). 11 % of the privacy statements mentioning direct marketing as a purpose offer an opt-in on the form, whereas 13 % offers an opt-out.

In total a quarter of the organizations having a privacy statement comply with this obligation. In addition, one third (30 %) asks the visitor, wishing to exercise his right of opposition, to contact the firm. This threshold is absent when directly offering the possibility to exercise this right in the form. One fifth (19 %) does not mention how the consumer can object.

All sites of the sample declaring that they will pass on the data to other organizations offer a right to object. This is a small group in the survey (14 websites). Half of the sites do not explain how one can stop the transfer of one's data. Some other sites refer to a postal or e-mail address. Finally, we observed that in one privacy statement the organization stated to contact the individuals if they intend to transfer their data to other parties. In that case permission will be asked.

### 4.3.5. Target group adaptation

As websites mostly dealing with kids and teens were studied, we checked whether or not information for parents is included in the privacy statement. Moreover, we investigated whether or not children are incited to ask their parents' advice before communicating their personal data. This is one of the recommendations adopted by the Privacy Commission. We found that 12 % of the privacy statements contain information for the parents. One out of ten privacy statements invites the child to ask the parents' opinion before communicating personal data online. One site asks the e-mail address of the parents to directly request the permission to store the child's data. Because only a small number of sites involve the parents, no comparison can be made between the different segments of the survey.

A next topic concerns the wording of the privacy statement. First of all, the information about the purposes of the database and the privacy rights has to be understood by the young visitor. Therefore, we checked whether or not the privacy statement was formulated without using (juridical) jargon and in a phrasing that we find adapted to the target group. Is a direct style used when the young internet user is addressed personally and is the language in harmony with the other content of the website? Conversely, is the style of the statement clearly distinguishable from the language used to attract the young visitors to browse through the other web pages? About half (48 %) of the privacy statements were presented in a way that could be comprehensible and appealing to youngsters.

Following table summarizes the proportion of statements giving information that has been made compulsory by the privacy legislation<sup>5</sup>:

Identification of person responsible <i>Who/what organization processes the data?</i>	52 %
Identification of the purposes <i>For what purpose(s) will the data be used?</i>	86 %
Right of access <i>Can the individual involved access his own data?</i>	67 %
Right to correct <i>Can the involved person correct possible errors?</i>	66 %
Right to object <i>If data will be used for direct marketing, can the person involved protest against it?</i>	60 %

Table 2: Information and rights mentioned in privacy statements

<sup>5</sup> More details and examples can be found in the full paper. The use of cookies and the answers to the mystery e-mails are also explained (Walrave, 2005).

## 5. CONCLUSION

A majority of the websites gathering personal data about, among others, children and adolescents, do not comply completely with the transparency principle and specific information obligations of the privacy law. Many websites do not meet with the compulsory information standards. A lot of websites have incomplete privacy statements and do not use a phrasing adjusted to the target group, while they do so in other segments of the website.

Hence we conclude that the under-aged apparently have less privacy rights on the Net when being asked for their personal data. The observance of the privacy law in other general surveys of commercial websites was relatively better. In previous surveys of websites we found a relative higher proportion of sites complying with these obligations based on the transparency principle of the law (Walrave, 2002: p. 28-29).

In brief, a marked trend is that some websites, dealing with minors (e.g. online contests, chatting and dating sites) ask for personal details about the visitors as well as about third persons (e.g. parents, friends) without giving any privacy guarantees. In some cases, websites requested data that are labelled as sensitive by the legislator, such as general data revealing racial or ethnic roots, religious or philosophical conviction and even data concerning sexual preferences (for example on chatting and dating sites). Such personal data are subject to very stringent rules, namely a principle prohibition of processing such data except with a few exceptions like the written permission of the person involved. In that and other cases parental consent is advised by the Privacy Commission. In only a few websites the young visitors are recommended to inform their parents or to ask their permission to fill in the online form.

Besides further investigation of the practices concerning the data processing in websites mostly aimed at minors, we also recommend a specific evaluation of the labels, technologies and other initiatives that have the protection of children and adolescents on the internet at heart.

The observations of the survey of the application of the privacy law in a sample of about three hundred Belgian sites aimed at kids and teens make the information and the sensitization of young internet users and their confidants of particular interest. This has to be done in different ways that addresses the segments among the young population in and outside the school environment.

The marketers who target young consumers with their campaigns on the internet and/or using mobile telephony have to be convinced about the concrete application of the privacy rights of the individuals who confide their personal data. This can be done on the base of specific legislative initiatives or co-regulation dealing with the possibilities and restrictions of the processing of data of the minors, possibly making a distinction based on the age of discernment for specific services designed for kids and teens. Also the creation of a ".kids" domain and/or a 'kids friendly'-label, including criteria concerning data protection, are interesting options.

Keeping the convergence of media in mind, some general and possibly technologically neutral principles have to be formulated, in a way as to apply to the explicit and implicit data processing. When, for which purpose(s), how and which personal data of minors can be harvested, must be made clear. How minors are informed about this and how they can exercise their privacy rights are important for the development and awareness of the growing-up consumers. Moreover, explanation is needed about the circumstances in which the advice/permission of a parent is indispensable. The US *Children's Privacy Protection Act* and other initiatives can inspire specific conditions for processing minors' personal data<sup>6</sup>.

Also, codes of conduct of the sectors targeting the youth and specific practical guidelines can be adopted by, amongst others, umbrella organizations and their members in order to find a balance between the service and the individual commercial communication towards young people, on the one hand, and the protection of their privacy rights, on the other. Only in such a way the young generation of ICT consumers can knowingly use it for different purposes.

## REFERENCES

- Bazsalisca, M.; Naïm, P. (2001), *Data mining pour le Web*. Solutions d'Entreprise. Paris: Editions Eyrolles.
- Dinant, J.M. (1999), *Les Traitements invisibles sur internet*. Namur: CRID, FUNDP, [<http://www.droit.fundp.ac.be/crid>].
- Internet Observatory (2003) *Opinion N° 1 concerning the protection of minors on the internet*. [<http://www.internet-observatory.be>]
- Milne, G. R.; Culnan, M. J. (2002), Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998-2001 U.S. web surveys. *The Information Society*, 18: 345-359.
- Privacy Commission (2002) *Advies Nr. 38 / 2002 van 16 september 2002. Advies uit eigen beweging betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op het internet*. [<http://www.privacy.fgov.be>]
- Walrave, M. (2002), *e-Privacy.be. Een betere bescherming van de privacy in Belgische websites, één jaar na het van kracht worden van de herziene privacywet? Een analyse van 250 Belgische websites m.b.t. het verzamelen van persoonsgegevens conform de Belgische privacywet (vergelijking 2001-2002) en een enquête bij webmasters*. Departement Communicatiewetenschap K.U.Leuven.
- Walrave, M. (2005) *Cyberkids' e-Privacy. Minderjarigen, minder rechten? Privacy Paper Nr. 4.*. Departement Communicatiewetenschappen. Antwerpen: Universiteit Antwerpen.
- 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.

---

<sup>6</sup> Cf. more information about the *Children's Online Privacy Protection Act* can be found on: <http://www.ftc.gov/bcp/online/edcams/coppa/index.html>, but also comments on: <http://www.epic.org/privacy/kids/>



Young people are increasingly enthusiastic users of the internet. Websites aimed at minors, often collect personal data during their visit. To protect personal data, legislative initiatives have been taken in the European Union. Moreover, institutions have made specific recommendations to protect children online. In order to check whether legal obligations were observed and recommendations applied, an online questionnaire was developed. Belgian websites mainly aimed at kids and teens have been analysed. The results show that, while a majority collects personal data, only a minority observes the privacy rights of the young website visitors and few involve parents when collecting personal data.

[www.e-privacy.be](http://www.e-privacy.be)

**Prof. dr. Michel Walrave - University of Antwerp – Communication Studies**