Kid's Privacy on the Internet
Nouwt, J.

Published in:
MultiMedia und Recht: Zeitschrift für Informations-, Telekommunikations- und Medienrecht

Publication date:
2002

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright, please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. Aug. 2019
KIDS’ PRIVACY ON THE INTERNET

COLLECTING CHILDREN’S PERSONAL DATA ON THE INTERNET AND THE PROTECTION OF PRIVACY

Dr. Sjaak Nouwt
Assistant Professor
Tilburg University, the Netherlands
Center for Law, Public Administration and Informatization

[Published in MultiMedia und Recht, Zeitschrift fur Informations-, Telekommunikations- und Medienrecht., 5(11), 703-709. November 2002]

Abstract
The children of today are growing up with the Internet. At the same time, there is a lot of uncertainty and ignorance about collecting personal data from children on the Internet, for example for direct marketing purposes. There is also much uncertainty and ignorance about the applicability of data protection rules. In this contribution, the American and Dutch legal framework for this phenomenon will be described. Furthermore, it appears that in EU member states, very little attention is being paid to this phenomenon. Obviously, there seems to be a lack of data protection regulation at EU level. The current evaluation of the EU Data Protection Directive 95/46/EC makes it possible to redress this deficiency.

Introduction
In the United States of America, the Annenberg Public Policy Center published several interesting reports about collecting children’s personal data on the Internet. The first Annenberg report The Internet and the Family, that was published in May, 1999 by the American Annenberg Public Policy Center, shows that over 75% of American parents are concerned that their children might give out personal information on the Internet. A second report The Internet and the Family 2000, published in May 2000, shows that 74% of American parents are still concerned that their children give out personal information on the net. A third Annenberg report, Privacy Policies on Children’s Websites: Do They Play By the Rules?, published March 28, 2001, shows that one year after the introduction of the Children’s Online Privacy Protection Act (COPPA), most children’s websites are still not following their legal requirements.1
The reports tell us that children very easily give out their personal data for a free gift. In fact, they give out their personal data, including data about their family life, much easier than their parents do. These personal data may also concern personal data about their family members, or the child’s social or economic situation. Both children and parents agree however, that children need their parent’s consent before giving information online.

In December 2001, the Dutch professor Patti Valkenburg (Children and Media, University of Amsterdam), published a book (‘Beeldschermkinderen’), in which she describes how commercial websites collect personal data from Dutch children. They collect data through cookies and distribute these data to other commercial websites that use this information for direct marketing. For research purposes, Patti Valkenburg communicated with the commercial websites and pretended to be a 12 year-old child. Her book caused concern by some Dutch Members of Parliament, who wanted to have this ‘problem’ immediately regulated by law. Apparently, even these Dutch Members of Parliament were unaware of the fact that the Dutch Personal Data Protection Act (2001) already regulates this kind of personal data processing.

Therefore, there seems to be a lot of uncertainty and ignorance about the collection of children’s personal data on the Internet, and about the regulatory framework to protect these personal data. That is why we will pay attention to this phenomenon in this contribution. Special attention will be paid to the legal framework in the USA and in the Netherlands.

United States: COPPA
In the USA, the collection of children’s personal data on the Internet is regulated in the COPPA: the Children’s Online Privacy Protection Act (21 April 2000). The Act prescribes that website operators are to describe when and how they have obtained verifiable consent from the parents, and what responsibilities the website operator has to protect a child’s online privacy and security. In the first place, the COPPA is applicable to commercial website operators and online service providers directed to children under 13 years of age. Secondly, the Act is also applicable to website operators of general audience sites who are knowingly collecting children’s personal data.

1 Joseph Turow, Privacy policies on Children’s Websites: Do They Play By the Rules? The Annenberg Public Policy Center of the University of Pennsylvania, March 2001.
The COPPA applies to the online collection of personal data from children under 13. Personal data means here: individually identifiable information about a child that has been collected online. Examples of such data are: full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The COPPA also covers other types of information, like hobbies, interests and information collected through cookies or other types of tracking mechanisms, which is tied to individually identifiable information.

To determine whether a website is aimed for children, several elements should be taken into account. Factors being considered by the US Federal Trade Commission are:
- the subject matter of the website;
- the visual or audio-content;
- the age of models on the site;
- the language used on the site;
- whether advertising on the website is directed to children;
- information regarding the age of the actual or intended audience;
- and whether a site uses animated characters or other child-oriented features.

To determine whether an entity is an ‘operator’ with respect to information collected on a site, several factors should also be taken into account. The FTC will consider, for example:
- who owns and controls the information;
- who pays for the collection and maintenance of the information;
- what the pre-existing contractual relationships are in connection with the information;
- and what role the website plays in collecting or maintaining the information.

Privacy policies
An operator of a website that is aimed for children must post a privacy policy or privacy statement on the home page of its website or online service, on its information practices, at each area where it collects personal information from children. An operator of a general audience site with a separate children’s area must post a link on the home page of the children’s area.

The link to the privacy policy must be clear and prominent. Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page, or a link that is indistinguishable from other links on the site, is not considered clear and prominent. In their report *Privacy Policies on Children’s Websites: Do They Play By the Rules?* (28 March, 2001), the Annenberg Public Policy Center suggests that the FTC should require website operators to place a distinctive “K” for “Kids” on their homepage on a specified place, for example at the top right corner. That would make it much easier for parents to find out if a website conforms to the COPPA. Secondly, the Annenberg Public Policy Center suggests that children’s websites should work together to create a standard privacy policy that allows for a quick and straightforward presentation of a site’s information-collection practices and the parents’ rights. These measures should make it easier for parents to find out if a website conforms to the COPPA and to read a website’s privacy policy more quickly. At the same time, these suggestions could make it easier for website operators to comply with the COPPA. The most recent report from the Annenberg Centre on this issue, shows that current privacy policies often prove very difficult to read, and are missing key elements.

According to the COPPA, the content of a privacy policy should consist of the following elements:
- the name and contact information (address, telephone number, e-mail address) of all operators collecting or maintaining children's personal information through the website or online service;
- the kinds of personal data collected from children and how these data are being collected (directly from the child or for example through cookies);
- how the operator uses the personal data (for marketing or notifying contest winners);
- whether the operator discloses personal data collected from children to third parties, and if so, in what kind of businesses these third parties are engaged, the general purposes for which the information is used, and whether the third parties have agreed to maintain the confidentiality and security of the information;
- the possibility for parents to agree to the collection and use of the child’s information without consenting to the disclosure of the information to third parties;

---
that the operator shall not collect more personal data from the child than is reasonably necessary to participate in an activity as a condition of participation;
that the parent can have access to the child’s personal information, ask to have it deleted and refuse to allow any further collection or use of the child’s information, and including the procedures for the parent to follow.

Parents have a right to access to the child’s personal information. At a parent’s request, website operators must verify the parents identity. A variety of verification methods may be used by the website operator. These verification methods can be the same as the ones that can be used to get parental consent.

Parental consent

The notice to the parents consists of a written statement or e-mail message to the parents, saying that the website operator wishes to collect or has collected personal data, including which personal data, on the Internet. The notice to the parents should also state that the consent of the parents is required for the collection, use and disclosure of the information and how the parents can provide their consent.

This parental consent should be verifiable. The website operator must take reasonable efforts to ensure that a parent of the child receives notice of the information practices and gives his or her informed consent to those practices.

When website operators want to disclose a child’s personal data to third parties, or make it publicly available, e.g. through a chat room or a message board, a reliable method of consent is required. Such methods include for example:

- getting a signed form from the parent via postal mail or facsimile;
- accepting and verifying a credit card number in connection with a transaction;
- taking calls from parents, through a toll-free telephone number staffed by trained personnel;
- email accompanied by digital signature.

However, when personal data are used for internal purposes a less rigorous method of consent is required. The website operator may use e-mail to get parental consent, or obtain a postal address or telephone number from the parent and confirm the parent’s consent by letter or telephone call.

An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. New parental consent is for example required when the operator who received parental consent for a child to participate in contests that require the child to submit limited personal information, now wants to offer the child access to chat rooms. New parental consent is also required when a website operator wants to disclose the child’s personal data to third parties who are in materially different lines of business from those covered by the original consent, like marketers of diet pills rather than marketers of stuffed animals.

The FTC uses a sliding scale approach to parental consent in order to allow time for reliable electronic methods of verification to become widely available and affordable. On October 20, 1999, the Commission issued its final Children’s Online Privacy Protection Rule implementing COPPA, which became effective on April 21, 2000. The FTC issued a final amendment to the Children’s Online Privacy Protection Rule to extend, until April 21, 2005, the time period during which website operators may use an e-mail message from the parent, coupled with additional steps, to obtain verifiable parental consent for the collection of personal information from children (only) for internal use by the website operator. The Commission will re-examine this issue through public notice and comment in connection with the statutorily mandated review of the Rule in 2005.3

Many website operators that provide popular online activities for children, are allowed to collect a child’s e-mail address without getting the parents’ consent in advance. These popular websites include, for example, contests, online newsletters, homework help and electronic postcards. Prior parental consent is neither required in the following cases:

- when an operator collects a child’s or parent’s e-mail address to provide notice and seek consent;
- when an operator collects an e-mail address to respond to a one-time request from a child and then deletes it;
- when an operator collects an e-mail address to respond more than once to a specific request, for example for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child;
- when an operator collects a child’s name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent and give him or her the opportunity to prevent further use of the information;

3 Federal Register / Vol. 67, No. 74 / Wednesday, April 17, 2002 / Rules and Regulations, pp. 18818-18821.
when an operator collects a child’s name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.

At any time a parent may withdraw his or her consent for collecting or using the child’s personal data. Parents may also ask website operators to delete the personal data that were collected from their child. However, if these data are necessary for the participation of the child in an online activity, like participating in a chat room, the website operator may terminate the service to the child.

The FTC has published practical guidelines for website operators and parents, about what website operators and parents should do to protect children’s privacy. 4

Case law
To enforce compliance with the COPPA, the FTC has been empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals in case of non-compliance with the COPPA principles. These enforcement mechanisms are based on its authority under Section 5 of the Federal Trade Commission Act. In fact, the Federal Trade Commission’s first Internet privacy case, GeoCities, was based on this Commission's authority under Section 5 of the FTC Act. 5 In that case, the FTC alleged that GeoCities misrepresented, both to adults and children, how their personal information would be used. The FTC prohibited GeoCities from misrepresenting the purpose for which it collects or uses personal identifying information from or about consumers, including children. The FTC ordered the company to post on its website a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, the FTC also ordered GeoCities to obtain parental consent before collecting personal identifying information from children 12 and under. 6

In another case, a children’s website operator agreed on February 13, 2002, to pay a fine and to place a hyperlink to the Federal Trade Commission’s online child privacy resources at each place where it collects information, in settlement of charges that the website violated federal unfair and deceptive trade practices laws and regulations promulgated under the Children’s Online Privacy Protection Act. The COPPA Rule, applies to commercial World Wide Web site operators and online services directed to children under 13, and to general audience websites and online services that knowingly collect personal information from children. The COPPA regulation requires that children’s websites get verifiable consent from a parent or guardian before they collect personal information from children, that they collect no more information than is necessary, and that they afford parents an opportunity to review and modify information collected about their children.

The FTC alleged, among other things, that American Pop Corn violated its website privacy policy by promising to collect the e-mail addresses of parents and inform them when they collected information from children and afford them an opportunity to invalidate their children’s registrations, but that it failed to collect the parents’ e-mail addresses or otherwise inform them of its information collection activities.

In addition to a $10,000 fine, the settlement obligates American Pop Corn, for a period of five years from the date of the decree, to place the following notice within its privacy policy, within e-mail messages to parents, and at each location where personal information is collected on its website:

“Visit www.ftc.gov/kidzprivacy for information from the Federal Trade Commission about protecting children’s privacy online.”

COPPA for teachers
Personal data are not only collected from children in a private sphere, like the family home, but also from students at school. At school, students are making use of the Internet more and more. The COPPA allows

---

7 United States v. American Pop Corn Co., N.D. Iowa, Civil Action No. C02-4008DEO, consent decree filed 2/13/02.
teachers to act on behalf of a parent by giving consent, but does not require them to do so. That is, the law does not require teachers to make decisions about the collection of their students’ personal information. The FTC advises teachers to check to see whether their school district has a policy about disclosing student information. If the teacher or parent does not consent to the collection, use or disclosure of the student’s personal data, the student’s participation in an online activity may be limited to areas of the site where the processing of personal data is not necessary. Even when consent is given, a teacher can still say no to having his student’s personal data disclosed to a third party. Consent by a parent or a teacher is not necessary if the website is collecting a child’s e-mail address only to respond to a one-time request for information.

A teacher may also decide whether to approve information collection from students based on new uses for the information. Website operators must let teachers know about the need for new consent by sending them a new notice and request. They will do this when they are changing the terms-of-use of the information in a ‘material’ or significant way.

A teacher may ask to see the information students have submitted. The site will ask the teacher to verify his or her identity to ensure that his or her student’s information isn’t given out improperly. Finally, a teacher must understand that he or she may revoke his or her consent at any time and have his or her student’s information deleted. To stop a website from collecting additional information from their students, teachers can revoke their consent. A teacher also may ask a site to delete any personal information it has already collected from his or her student.

The basic provisions of the COPPA and what they mean for teachers and their students are illustrated by the FTC’s Guide for Teachers: How to Protect Kids’ Privacy Online. A Guide for Teachers.9

Many school districts in the US are adopting Acceptable Use Policies (AUPs) to educate parents and students about Internet use and issues of online privacy and safety, and seek parental consent for their children’s use of the Internet. For example, an AUP may tell parents about the privacy policies of online services with which a school has contracts and students’ use of non-contract websites. It may include cautions against children disclosing personal information to websites, such as their full name, home or email address, and telephone number. Or it may tell parents that the school has established classroom email accounts rather than individual accounts if email communication is necessary between students and online services.

The bottom line for teachers is: look around. Many websites do not require children to provide any personal information to participate. Other sites limit their collection to personal information that is necessary for the activity.

Internet for Dutch pupils and students

The Dutch Ministry of Education, Culture and Science has commissioned The Knowledge Net project (Kennisnet), and is offering connections to institutions of vocational training and adult education, teacher training institutes, primary schools and secondary schools. The ICT Directorate within the Ministry is responsible for Kennisnet. It co-ordinates the process of connecting schools to the network.

The kennisnet.nl office within the Ministry produces the content for the Netherlands’ most important education domain.

Over 2.5 million people will be using Kennisnet in a year’s time. Each individual will have a unique log-in name affording them access to Kennisnet 24-hours a day, 7 days a week. By 31 December 2001, all pupils at Dutch schools in group 5 (primary year 5, for 8-9 year olds) and upwards, and all teachers and school heads will have access to Kennisnet. The Kennisnet website (www.kennisnet.nl) already provides access to several thousands of pages of information, designed or assembled especially for pupils, teachers, school heads and parents. All of these users have their own domain on the Kennisnet site. Work is now under way on a special domain for ICT co-ordinators. Of course, the World Wide Web offers much more information that is still appealing or interesting to Knowledge Net users, although it may not have been designed especially for educational purposes.

Users can access these pages easily via links, or search the Internet using the Kennisnet search facility. They not only have the option of ‘retrieving’ information on Kennisnet, they can also post it there. Every user can construct a website where he or she can post information suitable for use by other teachers and/or pupils. There are already various model lessons available on a variety of topics, and it would be difficult to find a novel without an extract somewhere on the Kennisnet. Another way of taking an active part in Kennisnet is to sign up for a discussion group. Incidentally, the Kennisnet community does not consist only of schools; parents, libraries, museums and school-related organisations also participate.

Protection of children’s personal data in the Netherlands

Contrary to the US, in the Netherlands it is not explicitly forbidden to collect personal data from children through the Internet (or otherwise). However, this does not automatically mean that collecting children’s personal data is always allowed. On the contrary: the Dutch legal system seems to be rather more severe than the COPPA. The COPPA is applicable to commercial companies and other organisations that collect children’s personal data through websites aimed at children of thirteen or younger, or through general audience sites which knowingly collect personal data from children. Personal data may be collected for a contest or when registering for an electronic newsletter. Despite the fact whether the data subjects (children and their parents) consider the collection of their personal data as an invasion of their privacy, there is no doubt that the collection of personal data is governed by the legal rules for data protection. ‘Personal data’ is any information relating to an identified or identifiable natural person. Because these personal data are being processed by automatic means (through the Internet), the Dutch Personal Data Protection Act is applicable.

Personal Data Protection Act

The Dutch Personal Data Protection Act came into force on 1 September 2001. The Netherlands implemented the EU Data Protection Directive EC/95/46 through this Personal Data Protection Act. Three principles are of special importance for collection and further processing of personal data. In the first place, there must be a well defined, and justified purpose for the collection of personal data (art. 6 Directive). In the second place, personal data may only be processed on legitimate grounds (art. 7 Directive). In the third place, further processing or the use of these personal data is only allowed when use is not incompatible with the purposes for which the data were originally collected (art. 6 Directive). Legitimate grounds are of eminent importance for the lawfulness of the purpose as well as for the lawfulness of further processing. Article 7 of the Directive contains six limited grounds for processing personal data. The first is the unambiguous consent of the data subject. The other five legitimate grounds for processing personal data are all based on the necessity principle. This means that in these cases, the principles of proportionality and subsidiarity are applicable. The principle of proportionality means that the invasion of the data subject’s privacy may not be disproportionate to the purpose for which the data were collected. The principle of subsidiarity means that the purpose for which the personal data are collected, cannot be obtained by other means that are less invading the privacy of the data subject.

The five other legitimate grounds for processing personal data are:

• necessary for the performance of a contract;
• necessary for a legal obligation;
• necessary for the vital interest of the data subject;
• necessary for the performance of a public duty;
• necessary for a legitimate purpose of the controller or of a third party to whom the personal data are distributed, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

It is obvious that the first four legitimate grounds are not applicable in the case where personal data are collected from children through the Internet. The last mentioned ground (legitimate purpose), prescribes that the privacy of the data subject should be considered. This means that the legitimate purpose for the controller has to be balanced against the data subject’s (the child’s) right to privacy. It should be obvious that the child’s (and the family’s) right to privacy should prevail, because children from whom their personal data are being collected, are hardly aware of the fact that their privacy, or the privacy of their family members, may be in danger when they supply their personal data to a website operator. Furthermore, according to the explanatory memorandum to the Dutch Personal Data Protection Act, the legitimate purpose for which the personal data may be processed should also be necessary for the performance of ordinary business activities. It must be impossible for the controller to perform his business without processing these personal data. It seems obvious to us, that this is not, (at least not always), the case where website operators collect personal data from children, even though we may consider marketing activities as ordinary business activities.

The only possible legitimate ground for processing children’s personal data is therefore the unambiguous consent of the data subject (art. 7, under a, Directive). However, the unambiguous consent causes problems concerning the processing of children’s personal data. Contrary to the EU Data Protection Directive, the Dutch Personal Data Protection Act has specific provisions for children. Article 5 of the Dutch Personal Data Protection Act requires the parent’s or other guardian’s unambiguous consent, when consent is required from children under 16. With regard to a child’s consent, it is interesting to compare Dutch civil law with the offline world. In Dutch civil law, a child is legally responsible for a contract when the child acts with the consent of his legal representative. In the Dutch legal system, consent is assumed when it concerns a child participating in a legal transaction, e.g.
buying sweets, or a book (an action considered common in society). If this is not the case, for example when a child buys a very expensive home cinema system, the legal representative of the child, e.g. one of the parents, may declare the transaction null and void. Because children are increasingly becoming common users of the Internet, a time may come that the collection of children’s personal data through the Internet will be accepted in society. However, we believe this time has not yet come.

Two types of consent
To understand the problem, it is important to realise that in this case we are dealing with two different kinds of consent: a contract law consent, and a data protection law consent. As stated above, according to article 8 WBP (art. 7 Directive) the data protection consent seem to be the only legitimate ground for this kind of processing of children’s personal data. This ‘unambiguous consent’ must meet the following criteria:

- The data subject must have freely expressed his wish; There is no question of free will if the data subject consented to processing under pressure of the circumstances;
- The data subject’s consent must be aimed at a specific processing of data. The processor must inform the data subject before he grants his consent so that the data subject understands what he is granting his consent for;
- The consent must be unambiguous. There may be no doubts about the data subject’s consent. The data subject may give his consent by ticking a box on an electronic form.

The burden of proof for obtaining the unambiguous consent lies with the website provider who collects personal data from children. This means that the website provider should be able to prove that consent was given and for what purpose. The website provider also has to prove that this consent was granted by the free expression of the data subject’s wish, and that he has informed the data subject sufficiently. Contrary to the case when a child buys a candy in the offline world, a web site provider may not assume that a child has given consent on the Internet, for the processing personal data.

Therefore, we conclude that the collection of children’s personal data on the Internet is not legitimate without the unambiguous consent of their legal representatives: mostly their parents, but sometimes their teachers. Contrary to the US, in the Dutch Personal Data Protection Act the age limit for children to give unambiguous consent is sixteen. In fact, the processing of children’s personal data in the Netherlands seems to be stricter than in the US.

Following the results of the research carried out by professor Valkenburg, several members of the Dutch parliament pleaded for separate rules for the protection of children’s privacy on the Internet. Based on the existing rules in the Dutch Personal Data Protection Act, this plea seems to be rather superfluous. However, it may be useful to take the children’s legal position into account when evaluating the EU Data Protection Directive. We believe that the American COPPA could be a good example for Europe.

Protection of children’s personal data in other European countries
In the meantime in Europe, the attention for the legitimacy of collecting personal data from children, although still small, is growing. An example illustrating the attention paid to this subject can be found on the website of the Jersey Data Protection Commissioner. To co-ordinate with the UK Government's drive to help raise awareness of the danger of paedophiles on the Internet the following information and advice is provided by the Jersey Data Protection Commissioner to parents and children:

For Parents:

- Keep the computer in a family room.
- Take an interest in what your child is doing on the Internet.
- Check that Privacy Policy Statements exist on sites to be visited and read them carefully.
- Decide whether to let the website collect personal information from your child.
- Ask to see any information your child submits.
- Don’t rely on filters. Whilst reassuring, they are often unreliable.

For Children:

- Never give your personal details such as name, home or school address, phone number etc.

---

• Keep your user ID and password private and secure.
• Look for Privacy Policy Statements on sites and don’t visit those without.
• Talk about the site’s Privacy Policy with your parents.
• Show your parents the sites you visit.
• Understand that Websites that request your personal details should get your parents permission before they collect it from you.
• Leave a site if it makes you uncomfortable or asks for more information about you than you want to share and tell your parents about it.
• Never arrange to meet up with someone you have been in contact with on the Internet unless you are accompanied by your parents.

The following links to Child Safety Websites are available on the Jersey Data Protection Commissioner’s website: National Society for the Prevention of Cruelty to Children (NSPCC)\textsuperscript{12}, Internet Watch Foundation\textsuperscript{13}, Childnet International\textsuperscript{14}, Chat Wise, Street Wise – children and Internet chat services, a paper prepared by the Internet Crime Forum IRC sub-group\textsuperscript{15}.

Another example of such a good initiative are the proposals of the French Commission Nationale de l’Informatique et des Libertés (CNIL), that were published in the CNIL report \textit{The Internet and the Collection of Personal Data from Minors}.\textsuperscript{16} Through this report, the CNIL wanted to draw attention to the lack of protection of children’s personal data. At the same time, the CNIL tried to develop a ‘best practice’ for the collecting of personal data from children.\textsuperscript{17} The CNIL proposals for such a ‘best practice’ relate to situations such as a child’s enrolment in a chat room or a forum, the use of children’s photographs on the Internet, contacts established with a website through e-mail or a newsletter, and the collection of personal data. When personal data are being collected from children on the Internet, the general rules for collecting personal data are applicable. Every electronic form that is being used for collecting personal data, should indicate the obligatory or optional nature or the fields that should be filled out, for example by using an asterisk. It should also be mentioned, that the data subject has the right to access, modification and rectification. Furthermore, the information on the electronic form should at least contain details on who controls the processing, the finalities of the processing and, where applicable, the right to object to the processing.\textsuperscript{18} What information should be provided to the data subject, when his personal data are being collected online, have also been explained by the Article 29 Working Party in the Recommendation on certain minimum requirements for collecting personal data on-line in the European Union.\textsuperscript{19} Whenever personal data are transferred to a third party, this should also be indicated on the form in such a way that the data subject can object to the transfer immediately, e.g by ticking a box. When the form does not indicate the transfer to a third party, it is assumed that the data is being used for internal purposes only.

In the case of minors, the CNIL adds the following conditions for the processing of personal data:
• The end-goal principle must lead the sites targeting minors to only collect data strictly necessary for achieving this end-goal;
• Any collection of data from minors concerning the family environment, parents’ life style and their socio-professional status must be considered to be excessive and unfair;
• It is prohibited to record data relating to racial origins, political, philosophical, or religious opinions, trade union membership or the customs of persons, without the express agreement of the latter (article 31 of the French law of 6.01.1978). The collection of such data from a child must be considered to be prohibited, unless the site manager can provide the proof that the parents expressly gave their consent;
• In no event should the implementation of a game or lottery designed for minors lead to the transfer to third parties of the data thus collected, if the site manager is not in a position to provide the proof that the parents have expressly consented.\textsuperscript{20}

\textsuperscript{12} NSPCC, \url{http://www.nspcc.org.uk}
\textsuperscript{13} Internet Watch Foundation, \url{http://www.iwf.org.uk}
\textsuperscript{14} Childnet International, \url{http://childnet-int.org/}
\textsuperscript{15} Internet Crime Forum, ‘Chat Wise, Street Wise – children and Internet chat services’, \url{www.internetcrimeforum.org.uk/chatwise_streetwise.html}
\textsuperscript{16} Internet et la collecte de données personnelles auprès des mineurs.
\textsuperscript{17} See p. 14 of the report.
\textsuperscript{18} Article 29 Data Protection Working Party, Privacy on the Internet - An integrated EU Approach to On-line Data Protection. 21 November 2000, WP 37, p. 47.
\textsuperscript{20} CNIL, The Internet and the collection of personal data from minors. 12 June 2001, p. 15-16.
Conclusion

The children of today are surfing more and more on the Internet. They are not just using the Internet in the private sphere, but also for educational purposes. Children are also a very interesting group of consumers from a marketing point of view. For this purpose it is obvious that personal data collected from children can be of great economic value. However, existing rules for the processing of personal data are applicable to the collection of personal data from children on the Internet. Recently, in the US these rules have been made explicit in a special regulation: the Children’s Online Privacy Protection Act (COPPA).

The Dutch Personal Data Protection Act, that has implemented the EU Data Protection Directive 95/46/EC, is also applicable to the processing of personal data, collected on the Internet. When collecting these personal data from children under 16, the only possible legitimate ground to process these data is the unambiguous consent, given by the legal representatives of the child.

At a European level, a specific legal framework for the processing of children’s personal data does not yet exist. However, in several European countries legal attention to this problem is growing. The omission of a legal framework might be a good subject for the current evaluation of the EU Data Protection Directive. For the sake of legal certainty, for data subjects and for controllers, it is preferable if the EU follows the American example and draft a COPPA at a European level, or at least insert a COPPA-like regulation in the updated version of the EU Data Protection Directive. In the meantime, European Data Protection Authorities can draft guidelines for the collection of children’s personal data on the Internet.