

Working Paper

Childrens' Privacy On Line: The Role of Parental Consent

adopted at the 31st meeting, Auckland (New Zealand), 26/27 March 2002

Introduction

Parental authorisation is often presented as part of a response to on-line issues affecting children and young people and this had been seen most explicitly in the Children's On-line Privacy Protection Act 1999 in the United States. However, questions have been raised as to how parental consent properly is to be seen in terms of privacy and data protection. Privacy involves the exercise of personal autonomy whereas parental consent might better be seen as reflecting a "best interest" or "child protection" model.

This paper does not attempt to canvass all on-line privacy issues for children and young people. It focuses on parental consent and related matters. Nor is it concerned with the merits or otherwise of requiring parental consent before ordering goods or services, which principally raises issues of consumer protection or contract rather than data protection.

In determining where parental consent might be required, it should be borne in mind that the purposes of consent, in a data protection context, is to protect the interests of the child not of the parent. Parental consent should not be a requirement where a child is capable of taking its own rational decision on the relevant matter. It should not be a mechanism through which a parent can override the child's decision unless there is a real risk the child does not appreciate the consequences of the decision or the child's naivety is being exploited. Essentially, parental consent should be required where it is in the interests of the child that a decision on fairly processing his/her personal data is taken but the decision cannot reasonably be left to the child alone.

There is some difficulty with translating general principles into practical rules. Not all children have the same ability at the same age. (This may be even more marked when a web site operates on a global basis.) For example, a standard set for a child 12 years and above may be overly restrictive for some children but insufficiently protective for others. On the other hand, a rule that simply states that a data controller must take the ability of a child into account in deciding whether parental consent is required is almost meaningless in practice. How could a data controller make such judgments unless it has an established relationship with the child? A vague rule will lead to different standards being applied in equivalent circumstances and is open to exploitation by unscrupulous traders. Even an age-based rule has problems. How, in the on-line world could a data controller know the age of a person accessing its website? Might the establishment of mechanisms to verify such details create privacy risks in other contexts?

Children might well be tempted to give wrong information if there is some perceived benefit that accrues from doing so. This does not mean that asking a child his/her age is of no value but the possibility that children will not tell the truth should be recognised and not exploited by data controllers. A cautious approach might be to ensure that the consequences of the decision not be such that there is a risk that a child who gives a false age will be exposed to totally inappropriate use of his/her personal data.

It has been suggested that unless parental consent is “verifiable” it is of no value. However, views differ on this point. Although a child can easily say that parents have consented when they have not, simply asking the question provides some (limited) protection. (Consider the off-line environment where most children will be wary of telling a teacher that their parents have consented if they might get caught out later.) There may be cases where asking a question and putting children in the position where they have to lie if they are to proceed without parental consent will be sufficient measure to ensure fair processing of personal data. However, in most cases where parental consent is the appropriate standard it is necessary for the consent to be verifiable. This is clearly difficult to achieve in practice. The fact that obtaining verifiable parental consent may be impracticable or require disproportionate effort should not place the child at risk. If a data controller is unable or unwilling to make the effort to verify consent, then this should not be seen as a reason for adopting a less restrictive standard. The consequences of the data controller's unwillingness must be that they can then only proceed as if consent has been denied.

When might parental consent be required?

In what circumstances might it be appropriate to obtain parental consent?

- where a child is asked to provide personal data - depending on the age of the child and the nature of the data controller's business this might be the provision of *any* information or only of *certain* information (such as sensitive data or that which is solely required to support marketing activities);
- where a data controller intends to disclose information about the child or use it for a different purpose, typically direct marketing;
- where identifiable information about a child is to be published on a website.

Generally it would not seem appropriate to require parental consent:

- to exercise a subject access right on-line.

Conclusions

The IWGDPT recognises that it is not possible to develop a single set of standards for the application of parental consent to the processing of children's personal data on-line that are clear, practical and applicable worldwide. Furthermore it considers that ethical business practices and the rigorous adherence to generally accepted data protection principles will diminish the need to resort to parental consent.

Nevertheless the IWGDPT takes the view that those processing personal data in connection with children's on-line activities should be guided by the following principle.

In a data protection context, parental consent should only be used as a mechanism for protecting a child's privacy where this aim cannot reasonably be achieved without involving someone to represent the child's best interests in decision-making. Typically this is a parent. Parental consent should

not be a mechanism to enable parents to exercise control over a child in circumstances where the protection of the child's privacy does not require the parent's involvement.

The IWGDPT makes the following suggestions to data controllers as a benchmark which will in many cases satisfy data protection requirements. The suggestions may need to be adapted in the light of the particular circumstances in which data controllers process children's personal data and the applicable national law:

- Where personal data are used to send communications directed at children (individuals under 16 years of age) or likely to be of particular interest to children, the communications should be age appropriate and should not exploit the child's credulity, lack of experience or sense of loyalty.
- Personal information should only be collected from children with the explicit and verifiable consent of the child's parent (including guardian or principal caregiver) unless:
 - the child is aged 12 years or over and
 - the information collected is restricted to that necessary to enable the child to be sent further lawful on-line communications and
 - the child understands what is involved.
- Personal information collected from children should not be disclosed to third parties without the explicit and verifiable consent of the child's parent.
- Personal information relating to other people (for example parents) should not be collected from children.
- The public display or distribution of personal information about children should not occur without the explicit and verifiable consent of the child's parent.
- Children should not be enticed to divulge personal information with the prospect of a game prize or similar inducement.
- Reliance on parental consent for processing a child's data should be time limited. When an individual ceases to be a child or becomes clearly capable of making the relevant decisions him/herself, processing should be based on the individual's own decisions not those of his/her parents.

A requirement to obtain a parent's consent does not override other requirements of applicable data protection law, for example

- A requirement to also obtain the child's consent
- Limitations on secondary use of the information provided by the child.