Children and young people and their right to the protection of their privacy

Summary

It should be considered both in relation to web sites and internet locations which are specifically designed for and consist very largely of children, and "mixed environments" where children and young people are found in great numbers but where they are nonetheless numerically in a minority as compared with adults. These different environments are likely to require different approaches.

1. Children and young people have data protection and privacy rights of their own which come into existence the moment they are born. These rights are separate from and independent of their parents.

2. Until a child or young person is old enough to comprehend the nature of the data transaction being put to them it will usually be necessary to obtain parental consent prior to collecting personally identifiable information from that child or young person. This will be especially important where the personally identifiable information might impact on the child's personal health or safety, be used in relation to any commercial setting or where the data may be used in other ways which are sensitive.

3. Parents' or guardians' wishes in respect of data protection and privacy issues may not always coincide with the best interests of the child. Where that is the case the best interests of the child should always prevail.

4. Online service providers have a duty of care which is owed directly to the children and young people who are their members or who use their services.

5. Online service providers are not entitled to assume that simply because a parent or guardian or some other entity is paying for the service or has given permission for a child or young person to join a service, that they have therefore assumed total or sole responsibility for ensuring that the child is aware of the site's data collection or privacy policies.

6. It is widely acknowledged that very many adults of average intelligence, average levels of numeracy and literacy have difficulty digesting and understanding a great deal of what web site owners present to them as their terms and conditions or policies on data collection and privacy. Thus if a web site which allows persons as young as 13 to be members, but still presents all of the information about its data collection and privacy policies in a uniform way for all users, it is unlikely to be properly discharging its obligation to ensure that all of its users have given informed consent to personally identifiable information being collected about themselves.

7. Communicating information about privacy settings and data protection policies generally for children and young people can be promoted by using pictograms which alert users to important aspects of the default settings and point to sources of accessible information about the consequences or advantages of varying from the default settings.

8. It is very well documented that substantial numbers of children and young people who are below a site's or a service's stated minimum age nonetheless use those services. Thus through their continued refusal to obtain sufficient, accurate information about their users, most online services have failed to develop and deploy robust age verification mechanisms. This can be commercially advantageous to these companies. It can also put children and young people at risk in more than one way.

The Rights of Children and Young People to data privacy and protection

Children and young people share all of the same rights to data privacy and data protection as adults, and they acquire these rights the moment they are born. However it is well established that children are also entitled to extra layers of protection to help guard against potentially harmful intrusions by third parties who might otherwise take advantage of their innocence or naïveté, thereby putting them at risk. This risk might relate either to their personal health or safety or to the potential for them to be exploited for commercial purposes.

Furthermore it is important to recognise or remind ourselves that children's and young people's rights to data privacy and data protection reside with them as individuals. Their parents or guardians can act as agents or in some cases must consent to certain matters but they do so only in so far as it is in the best interests of the child and normally only in so far as, at the relevant time, the child is incapable of giving informed consent because they do not fully understand the implications or consequences of acting in one way or another or of understanding the implications of taking one decision rather than another. This makes it a subjective test, to be applied child by child in each and every individual case.

Herein lies a major problem. eNACSO knows of no way of administering a subjective test, case by case, child by child, in the online environment. Much less is there a way of doing this as part of a remotely administered routine process or as a prelude to a company or other organization deciding whether or not to engage with a child in some way or other. Whatever view one might have as to the desirability of such a practice, it will not happen within the foreseeable future.

Individual assessments of a child's or a young person's abilities are most definitely a better and preferred way, and in real world situations it is important to keep them as the core principle. But in the online space it is a counsel of perfection which is of no practical use at all.

Children's web sites

There are a range of sites which are expressly aimed at children and young people. Some are designed for very young children. Many of these sites are subscription based and therefore historically typically have depended upon parental engagement, if only to provide a means of paying the subscription.

eNACSO is not aware of any major studies which look at how sites or services which are specifically for or are mainly used by young children present their terms and conditions, including information about their policies and procedures on data collection and privacy, either to parents or children, or both. The rights of the child may not always be co-terminus with those of their parents, even in relation to a service that is being paid for by the parent.

Irrespective of who pays for a service, or whether or not parental consent has been obtained to allow a child or young person to use a service which is free at the point of use, online service providers continue to have a separate and independent duty of care which is owed directly to the children and young people who are their members or who use their services. Online service providers are not entitled to assume that simply because a parent is paying for a service or has given permission for a child or young person to join a service that the parent has therefore assumed total or sole responsibility for ensuring the child is aware of the site's data collection, privacy or other relevant policies.

Moreover, as more and more children, even very young children, acquire a capability to pay for things themselves e.g. through the increased availability of prepaid credit cards and online gift cards, it is possible that children's sites may need to consider the possibility that young children are joining entirely under their own steam without there necessarily having been any parental engagement[3]. Thus information on privacy, or the site's terms and conditions generally, prepared for and presented to an audience which is assumed to be composed entirely of adults (in their capacity as parents), may not be sufficient to discharge the site owners' legal obligations to all of its members.

eNACSO appreciates that some sites have experimented with developing simplified versions of their main terms but we are not aware of any expert or independent evaluation of how widespread or effective these have been, either generally or specifically in relation to the position of sites designed exclusively or overwhelmingly for children.

Web sites used by children and adults

Perhaps the largest single class of online service providers that are important to vast numbers of children and young people are the social networking sites, of which Facebook is the leading exemplar. These are essentially mixed environments i.e. whilst there are substantial numbers of children and young people on them, the great majority of members are aged 18 or above[4].

It is widely acknowledged that very many adults of average intelligence, average levels of numeracy and literacy have difficulty digesting and understanding a great deal of what web site owners present to them as their terms and conditions or policies on data collection and privacy. The same is true in relation to how they explain the site's privacy settings or how to change them.
Thus if a web site which allows persons as young as 13 to be members but nonetheless presents all of the information about its data collection, privacy policies and settings in a uniform way for all users, it is unlikely to be properly discharging its obligation to ensure that all of its users have given informed consent to personally identifiable information being collected about themselves. This is not compatible with a principle that is central to European data protection and privacy laws.
In the previous section on children's web sites it was observed that some sites have experimented with developing simplified versions of their main terms but there does not appear to be any expert or independent evaluation of how widespread or effective these experiments have been. The same stricture applies in relation to mixed environments.

However, no discussion of this subject would be complete without consideration of the position of "unauthorised users". Many sites specify 13 as their minimum point of entry but it is well known that large numbers of children below that misrepresent their age in order to be able to open up an account[5]. Because these sites know, or ought to know that they have substantial numbers of users who are below the age of 13, a question arises as to what duty of care the sites owe to them?
Some social media sites say that whenever they detect sub-13 year old on its site it deletes their account but there is no independent evidence on this and whatever they do is doing it obviously is not working very well because the numbers of sub-13 year olds who are members remain very high.
Failing to collect certain information can be a deliberate policy. Such an omission can work very much to a company's commercial advantage. Thus, through their continued refusal to collect sufficient, accurate information about their users, online services have denied themselves the means to develop and deploy age verification mechanisms. In the face of all the evidence, are they entitled to remain wilfully ignorant? What is the point of specifying a minimum age limit if in practice not enough is done to enforce it?

Greater certainty needed in the modalities

Whilst it is vital to have clarity about the basic legal principles governing the area of privacy, it is equally important to be clear about how, in practice, these rights should be given expression.
eNACSO appreciates that every company wants to develop its own distinctive branding and its own specific relationship with its customers but with matters such as privacy there is considerable merit in the regulatory authorities insisting that companies develop a consistent approach that all consumers will quickly come to recognise and understand. Moving between web sites should not mean having to learn a whole new vocabulary or set of concepts for dealing with privacy. There are lots of other ways companies can be distinctive.
In specifying the modalities of communicating information about privacy settings and data protection policies generally for children and young people, if not others, it may be worth supporting specialist projects such as that being developed by the Netherlands Organization for Applied

Scientific Research to create pictograms which alert users to important aspects of the default settings and point to sources of accessible information about the consequences of varying from the default settings.
A definition and a method of determining what constitutes a children's or young person's web site or other area of online activity which is specific to or targeted at children and young people may need to be agreed and established as a standard which all regulators and self-regulators could integrate into their national or local codes in relation to data collection and privacy practices. Consideration may also need to be given to developing particular rules for the same practices in "mixed" locations i.e. sites or areas where children and young people are in a minority but where it can be shown they are nonetheless present in substantial volumes.

Creating a definite lower age

In Spain and the USA laws have been passed which, at least in principle, establish a much clearer position in important respects. They appear to acknowledge that in an online environment carrying out a subjective test of a child's capacity to understand the nature of certain data transactions cannot be adequately determined. The Spanish law states that below the age of 14 companies must obtain verifiable parental consent before they can accept a child's data as part of a sign up process for an online service. Blunt and crude though it may be, in relation to the internet eNACSO can see no alternative but to follow the example of the USA and Spain.
A minimum age should be specified and given the force of law. Above this age, in the absence of any specific information indicating there is a need to enquire further, companies would not be obliged routinely to seek prior permission from parents before collecting or storing data from young persons. Below that age they always would. There is no suggestion that changing the law for the purposes of the internet or other remote environments need have any impact at all or require any alteration to the current law applicable in any situation where the child is visible to or in the presence of a doctor, teacher, or the vendor of a product or service. In those instances the existing laws and rules would still apply. Either way, in matters such as these companies need clarity and consistency.
Exactly what the minimum age should be ought to be the subject of consultation and fresh research. It may turn out to be somewhere around 12 – 14. On the other hand it may be more closely aligned to what is happening in the field of online commerce. This latter consideration is very important. So much of what is driving the internet is related to commercial activity of one kind or another. Thinking about data collection and privacy in the abstract, outside the commercial context in which it is being collected and the purposes for which it is intended, makes little sense. From a brief survey eNACSO has carried out we are aware that whilst there are significant differences between EU Member States in relation to some of these matters there also many points where their policies and practices coincide in relation to online data protection for children and young people. There are also many similarities in the ages at which children and young people might lawfully purchase different products and services, both offline and online.

A journey to adulthood

Children and young people are on a journey towards adulthood. Their bodies may not be suited to the consumption of certain products e.g. alcohol, or it is thought they lack the necessary judgment to be able to handle a range of items safely e.g. larger knives. Alternatively legislators have taken a view that some activities e.g. gambling should only be available to adults, or they have decided that particular types of material e.g. pornographic videos or violent computer games should only be sold to adults. Every EU Member State has regulations or laws of some kind which restrict the sale or provision of certain goods or services to persons below a certain age.
Young people down the ages have always sought to challenge conventions and test boundaries. Risk taking, rebelling against or seeking to manipulate "the rules" is in varying degrees a perfectly normal part of the process of growing up. The fact that the rules are sometimes broken, or it is difficult to

make them work always wholly as intended, is no reason for abandoning them altogether, or for giving up on the attempt to enforce them when necessary.
Rules, particularly rules backed up by laws, are a reflection of societal norms and values. They shape and influence behaviour and expectations, even in the breach. Equally the absence of rules implies permission, endorsement, consent or acquiescence of some kind.
In the case of age restricted goods and services available online the internet provides an easy way of evading the legally required visual age checks that are standard in real word establishments in cities, towns and villages. With a few notable exceptions it appears that the great majority of online retailers in Europe, active in many different markets, make no serious efforts to determine the actual age of persons attempting to buy age restricted products or services from them. This means they are regularly breaking the law and they must or ought to know it. Their acts of omission are putting children at risk.

Licensed to sell age restricted goods?

No retailer is compelled to sell anything online but if they are going to choose to sell age restricted goods then they should only do so if they are in a position to demonstrate that they are doing it legally. It is quite wrong for retailers, essentially, to make a calculated decision to take no action in relation to the online sale of age restricted goods or services knowing that the weak nature of the enforcement regime, the trivial nature of the fines and continuing lack of media attention means they have little or nothing to fear. As online shopping grows, as it becomes easier and quicker to pay for things over the internet, if action is not taken sooner, it is likely to be harder to put it right later.
Unless online retailers show they are making a determined effort to resolve this problem within a reasonably expeditious timeframe then governments should step in to establish a licensing regime. A licence would only be given to a company that could show it had a robust online age verification system in place. There would then be no need for a complicated enforcement action to be brought against offenders. The licence would be the key. Trading without one would constitute an offence. A hefty fine, or worse, would act as a major incentive for companies to comply.
A company should not be allowed only to ask a person to confirm their age by ticking a box on an internet page. However, having made good faith efforts to verify a person's age, if a company is still deceived and sells or supplies a product or service to someone below the legal age, the company should not be liable either in civil or criminal law.

eNACSO, 2011

Notes

[1] Many of the cards are marketed as being usable by persons of "any age".

[2] "EU Kids Online" shows that, in the 23 countries that participated in the survey, 21 of which were EU Member States, 60% of all 9-16 year olds use social networking sites and 57% report having their own profile. There appears to be little variation either by gender or by the socio economic status of parents. There is some variation by country with the highest, Holland, recording 78% usage of social networking sites by 9-16 year olds, Germany showing 50% and Romania the lowest at 47%. In some countries the spread of Facebook is such that in all probability its demographic closely corresponds with the general demographic of internet users in the nation.

[3] In the UK, for example, over 20% of all children between the ages of 8 and 12 had Facebook accounts.