January, 2011

eNACSO European NGO Alliance for Child Safety Online

Contents

Executive Summary -

1. - Online privacy touches upon key aspects of everyone's health, safety and personal development. Thus how online privacy policies and practices are presented and explained to children and young people below the age of 18 is of enormous importance. It is a subject that deserves special care and attention from all online service providers.

2. - Clearly the matters covered by "Protecting Consumer Privacy in an Era of Rapid Change" ("the FTC paper") and the COPPA Rule review are not coterminous but in relation to the specific interests of children and young people there is a considerable degree of overlap in a number of areas. Since the COPPA Rule review has not yet been completed perhaps inevitably the Era of Change paper is notably inconclusive in those respects.

3. - Moreover we were surprised to see no discussion in the FTC paper of the implications of the work being undertaken to develop a "National Strategy for Trusted Identities in Cyberspace", sponsored by the White House and the Department of Commerce. In a consultation paper issued in June 2010 there are several references to authentication and privacy enhancing technologies, some of which expressly highlight the question of how to authenticate the age of the user or person attempting to secure a product or service online.

4. - In contrast to the bulk of the FTC paper, where a series of admirably clear comments and proposals are presented, when it comes to children and young people, as well as other vulnerable and sensitive users, the paper largely seeks responses to more questions.

5. - eNACSO appreciates the need to "get it right" for the middle majority or mainstream internet users, but our view very much is that it is just as important, perhaps even more important, to "get it right" for those most likely to need extra help or consideration. Indeed "getting it right" for them might impact upon or have implications for the others so it may be unhelpful to divorce the issues or split them up in the way implied by the FTC paper.

6. - In very many European countries 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.

7. - Until a child or young person is old enough to comprehend the nature of a data transaction that is 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.

8. - When acting on behalf of their offspring in such matters a parent or guardian must always be guided by the best interests of the child. This will be especially important where the information being collected might impact on the child's personal health, safety, be used in any commercial setting or where the data may be used in other ways which are sensitive.

9. - Online service providers are not entitled to assume that simply because a parent or guardian or other entity is paying for a service or has given permission for a child or young person to join or use a service, that the parent, guardian or other entity has therefore assumed total or sole responsibility for ensuring that the child is aware of the site's data collection or privacy policies. Online service providers have a separate, continuing and independent duty of care which they owe directly to the children and young people who use their service. This has implications for how information about privacy policies and practices are presented on sites which are overwhelmingly used by children.

10. 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 -

online service providers present to them as their terms and conditions or policies on data collection and privacy. Where a web site allows and has significant numbers of children and young people as members or users, but nonetheless it presents all of the information about its data collection and privacy policies or privacy settings in a uniform way that is aimed at adults, it is unlikely to be discharging its obligation to ensure that all of its users or members are properly informed. Perhaps special guidance is needed to assist sites which operate these kinds of mixed environments.

11. Whilst appreciating that companies wish to develop their own distinctive branding and relationships with their customers, particularly younger users should not have to learn a whole new vocabulary in relation to privacy simply because they check in to a new site. Some degree of standardization in relation to how information on privacy is communicated is essential. In that connection special attention needs to be paid to how such information is conveyed to children and young people.

12. The failure or deliberate refusal of sites to obtain sufficient, accurate information about members or users can create safety risks.

13. Many sites know, or ought to know, they have substantial numbers of children and young people who are members or are using their services even though they are below the stipulated minimum age. In the UK around one in five of all 8 to 12 year olds have accounts with a well-known social networking site, even though its minimum age is 13.

14. The operation of the COPPA Rule may provide companies with zero legal incentive to determine the actual age of users but that does not make it ethically right for such companies to refuse or persistently fail to act to correct a known large scale breach of their age policy. They should not hide behind COPPA immunity.

15. If a company knows a whole class of persons are consistently and regularly on its site, even if strictly they are there outside their standard terms and conditions, that company still has a duty of care towards them.

16. It is in some sense a deceptive practice for companies to continue to market their services stating they are only intended for people above a certain age when they know perfectly well they are incapable of guaranteeing or enforcing the policy with any degree of efficacy. Moreover it is very hard to see how this state of affairs can be consistent with good data protection and privacy practice.

17. A data controller should not be allowed to remain willfully ignorant of what they themselves proclaim to be a key fact. If age is irrelevant to their service then they should not collect data about it or limit the service by reference to it. But if the company says age is important they should collect age data, and do it with a degree of professionalism. They should be able to repose a reasonable degree of confidence that their data will be accurate and their stated policy is working in the way they say it is intended.

18. In effect all that is being suggested here is that a much greater effort is needed to find better ways to reflect online practices such as age verification which are taken for granted and are very widely observed in the real world. The idea this cannot be done or that it can only be done in a way which increases dangers to children and young people is simply implausible.

19. Whilst appreciating there are substantial practical difficulties associated with constructing a secure system that would allow age verification to work with a high degree of confidence both as to its accuracy and efficacy, the whole of the internet is in one sense a testament to defeating many seemingly enormous, even apparently insuperable challenges.

20. The way the debate on age verification took place in the USA following the cases involving MySpace was most unfortunate. There is a lot more to age verification than an (impractical) hope that it can be used to deter paedophiles from contacting children who use social networking sites.

21. In the long run the present system is not sustainable. The potential to abuse anonymity, the refusal or inability to authenticate important data about people in environments where it matters, lies at the heart of many of the internet's larger and enduring problems. The sooner everyone gets on with putting that right the better it will be for children and young people around the world. The "National Strategy for Trusted Identities in Cyberspace" is very clear about the privacy and other gains to be had from improved online authentication systems and we commend them for it.

22. Given the meteoric rise of online retailing and online behavioural advertising it no longer makes sense to divorce the question of advertising and online sales practices from the data collection processes and privacy practices on which they depend. Special attention should also be given to unlawful online sales of age restricted goods and services.

23. The privacy policies and practices of major US based internet companies are of profound importance to children and young people in very many overseas jurisdictions because the US defaults tend to become the global defaults.

24. Getting US companies to shift from the US determined defaults to reflect local laws overseas can sometimes be a protracted and hence expensive process. Thus US Federal law ought to be changed to make it a requirement that before a US company commences online operations in a foreign jurisdiction its policies and procedures should at the outset comply in all material respects with local requirements. Where is a conflict of laws a mechanism for identifying and reconciling them should be established as part of the in-country start up process. It should not be left to the police, NGOs or others to discover there is a divergence and then have to negotiate a change after the company has begun commercial operations. This ought to be part of the standard due diligence but we are aware that it is not.

Part One : the rights of children and young people

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. This position is reflected in the laws of all or most EU Member States.

However, it is well established that children and young people 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, to their future employment or educational prospects, or to the potential for them to be exploited for commercial purposes. For this reason the issue of online privacy and how it is addressed is now seen as being central to the wider online child safety and child welfare agenda.

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. In some European jurisdictions 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. For these reasons eNACSO commends the US practice of fixing a minimum age, below which it will always be necessary to obtain verifiable parental consent, although the fact that there is no system in place to ensure this rule is honoured does detract somewhat from its appeal.

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.

One of the largest sites for very young children is "Club Penguin". When Disney acquired it in 2007 they were reported to have paid US$700 million, underlining the highly commercial nature and magnitude of the economic interest in children's and young people's activity online[i].

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[1].

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[2]. 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. However, on the face of it this looks like a promising avenue. The Netherlands Organization for Applied Scientific Research has been engaged in some interesting work to create pictograms which alert users to important aspects of the default privacy settings and pointing to sources of accessible information about the consequences or advantages of varying from the default settings.

---

[1] In the UK, for example, child tracking services provided through the GSM network by mobile phone companies, normally are paid for by a child's parent, but the child nonetheless has an absolute, unconditional right to cancel the service unilaterally at any time. If they give notice the service stops immediately. There is no parental override. Similar services supplied in some countries outside the EU e.g. in the USA, are understood to provide for a parental veto or require parental consent for the service to be stopped or altered. Terms like these, if applied in a blanket way to all children under all circumstances, would probably be unlawful in all or most EU Member States.

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

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[3].

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 allows children and young people 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 discharging its obligation to ensure that all of its users are properly informed.

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[4]. Because these sites know, or ought to know that they have substantial numbers of users who are below the age of 13, eNACSO believes they owe a duty of care to them.

Facebook says that whenever it detects sub-13 year old on its site it deletes their account but there is no independent evidence on this and whatever Facebook is doing it obviously is not working very well because the number of sub-13 year olds who are members remains very high.

Failing to collect certain information may 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 nothing is done to enforce it? COPPA notwithstanding is this not in some sense a deceptive practice? Companies should not hide behind their COPPA immunity.

[3] "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.

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

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, particularly younger ones, 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.

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.

Part Two: the economic dimension to the internet

In what follows we present data which was derived principally from the UK. Whilst there will, of course, be substantial variations between EU Member States there can be little doubt about the direction of travel in relation to the EU as a whole.

A report commissioned by Google and published in October, 2010, "The Connected Kingdom[ii]", suggests that in 2009 the internet contributed £100 billion, or 7.2% of GDP, to the UK economy. This made it larger than construction, utilities, transportation and several other long established industrial sectors.

In 2009 approximately 250,000 people were employed by e-commerce companies and the report says the value of the UK's internet economy is expected to grow by 10% per annum until it reaches 10% of GDP by 2015.

The "Connected Kingdom" report discusses some of the methodological challenges the authors had to confront when assembling their data and making their findings but the burden of its principal conclusions cannot be in doubt. The internet is not only now central to many aspects of the UK's social life it is also of enormous and growing importance to our national economy.

The recent growth in online retailing provides more evidence for the latter proposition. An ever larger share of retail activity is expected to continue to shift to online environments[iii]. In August 2010 UK shoppers spent £4.4 billion online, up 15% on August 2009.[iv]

Moreover the level of economic activity which in one way or another is tied to children and young people is sizeable.

In 2006 children and young people in the UK up to the age of 19 spent £12 billion from their own pocket money or earnings derived from part-time jobs. When one adds to the equation the amounts spent by parents on their children, over which in varying degrees children and young people have some influence, in the same year the total value of the market increased to almost £100 billion[v]. In February 2010 it was estimated that on average it costs a family in excess of £200,000 to see each child through to their 21st birthday[vi].

This loosely defined but large children's and young persons´ market is therefore of major economic significance, not just to individual firms competing for parts of it, but also for the wider economy. The size of the market also helps explain why so many companies are interested in it.

The example of Disney's acquisition of "Club Penguin" was referred to earlier. Further direct evidence of the importance attached by internet companies to children and young people as actors in the economic space emerged in a recent article in the "Wall Street Journal"[vii].

Advertising – a key building block

The Wall Street Journal's investigation focused on the use of "cookies", "beacons" and other tracking technologies. Typically these collect information about the web sites a person visits and the kinds of things they do when they are on them.

Your browsing habits say a lot about you and your tastes. This is precisely why these data are so valuable and so sought after by advertisers. As the Journal observed, the data can cover

> age, tastes, hobbies, shopping habits, race, likelihood to post comments and general location, such as city.

It is because of tracking technologies, or in some cases information derived directly or expressly from the individual, for example in their profile or through their postings, that when they go online and fire up a web browser or sign in to the service they straight away find ads served up to them which mirror their recent online activity and wider interests. This practice has become known as "online behavioural advertising", usually shortened to "OBA[5]".

The justification for OBA is eminently reasonable. It is meant to ensure that an individual is not plagued with advertisements for things they are not interested in and would never buy.

To the extent that such practices help reinforce people's existing patterns of behaviour there could be a downside to OBA, but the upside is also very clear. The major problem with OBA lies in its intrusiveness, its reliance on data which is all about you as evidenced by what you do when you go online. That is why the question of informed consent is so important and why the ability to decline any involvement with OBA is also vital.

The companies collecting the data which is used in OBA maintain that they separate them from anything that would allow an individual internet user to be traced or identified by any process of reverse engineering but that view does not go uncontested[viii] and anyway it is not entirely or the whole point. Companies do not have a unilateral right decide that they can take an individual's data and profit it from it without that individual's express consent. That should apply to children and young people just as much as it should to adults.

Companies such as Google and Facebook collect these data and retain them. They do not sell them on or provide them to any third parties. The data form the basis of their offer to advertisers. Other companies collect the data and sell them. The Wall Street Journal discovered one list available for sale to advertisers going under the soubriquet "Teeny Boppers".

Children's web sites and children's data

The Wall Street Journal's investigation revealed that

> popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults

The article looked at 50 sites that were popular with American "teens and children". Media giant Viacom owned eight of the 50 sites. The sites in question were all associated with Nickleodeon TV, a channel aimed squarely at younger children. They also looked at 50 of the most popular US sites which were principally aimed at adults.

The children's sites had placed 4,123 tracking devices on to the computers which had accessed them. This was 30% more than were found on the adults' sites. Google seems to be the single most active company in relation to placing tracking tools on sites principally used by children.

---

[5] The sustained growth of online behavioural advertising suggests that a significant and still growing proportion of *all* online advertising is linked to online data collection about individuals. One IAB estimate suggests that in 2009 80% of all online advertising campaigns "involved tracking of some sort". An industry commentator observed

> The advertising business, in short, loves online tracking just about as much as privacy advocates hate it.

A specific example cited in the Journal article concerned a 10 year old child who reported that Google consistently presented her with ads for "pets… 'virtual worlds' and 'online goodies' such as little animated graphics to decorate a website".

Many companies say they make no attempt to collect data which is *solely* about or of interest to children, moreover the constraints imposed by the rules about advertising to children still apply, or ought to[ix]. Accepting in good faith that in the above illustration Google did not knowingly target the child, did not engage in intentional behavioural advertising aimed at children or did not deliberately collect data which was only likely to be of interest to a child, it has to be said that they might as well have done. The end result was the same.

The fact that companies go to such lengths to obtain the kind of data discussed here from web sites most commonly frequented by children and young people is very telling. It shows beyond any shadow of a doubt that children and young people are economic targets on the internet, just as they are in the real world.

The UK's Internet Advertising Bureau (IAB) rules[x], prescribe 13 as the minimum age for which "segments" of OBA can be created. It is not entirely clear whether or how this aligns with rules issued by other regulators or trade bodies with an interest e.g. the Advertising Standards Authority (ASA) and the Direct Marketing Association (DMA) where 12 is given as the minimum age at which information can be collected without prior parental approval.

In research carried out for the UK's Office of Fair Trading[xi], "Attitudes to Online Markets, Report by FDS International" (FDS Report)[xii], at para 9.16 it is revealed that 37% of the sample were either "very concerned" or "somewhat concerned" about cookies. That is a big number. If the same survey question was asked again but it was preceded by an explanation of how cookies work in relation to children and young people it must at least be a possibility that the percentage would come out even higher.

It is true that it is always possible to block cookies and beacons or to get rid of them[xiii], and the IAB rules, for instance, expressly say that adherents to their code must provide a

> clear and unambiguous notice to users that it collects data for the purposes of OBA. This notice shall include information about what types of data are collected, how these data are being used and how users can decline OBA…

However, companies that use these technologies vary enormously in the effectiveness, amount of time, energy and resources they devote to ensuring their customers, users, or web site visitors are fully briefed in the way the IAB rules clearly intend. Not everyone makes it equally easy to avoid OBA.

Cookies and similar tools predate OBA by many years and they are not only used as a means of supplying data that ends up in an advertiser's database. There is no doubt that cookies can be very useful and save internet users a great deal of time, but some companies appear to be taking unfair advantage of that fact. They seem to rely on consumer exhaustion or perplexed frustration to get their customers, users or web site visitors to set their browsers always to accept cookies or to opt for the default settings, or just to click "yes". The default settings or the "yes" click typically are calculated to maximise or at any rate to enhance the company's revenues. Using complexity and fatigue to bamboozle consumers is common in many markets but it is inexcusable in all of them.

Children are economic targets

As we have seen, children and young people plainly are economic actors and economic targets on the internet, as they are in the offline world. This ought to be explicitly recognized and incorporated

into future policy making, both generally but also specifically in relation to policy around tracking technologies and the advertising, data collection and privacy practices which they facilitate.

Children and young people are of course entitled to participate in economic activity, online and off. Indeed they need to do so as part of the process of growing up, learning how to handle money, and anyway within reason it can be a lot of fun. However, many of the rules and practices which have been established to protect children and young people from unfair commercial practices in the real world e.g. about encouraging excessive or inappropriate spending and "pester power" do not yet seem to have been fully translated into the virtual space or to have found an online equivalent or proxy.

Given the meteoric rise of Online Behavioural Advertising (OBA) it may no longer be satisfactory or make sense to divorce the question of advertising and online sales from the data collection processes and privacy practices on which an already substantial proportion of it is based, particularly in relation to the way OBA and online selling impacts on children and young people.

Regulatory concerns

The UK's Office of the Information Commissioner, the Commission of the European Union, national Governments both in Europe and elsewhere, the Article 29 Working Party[xiv], as well as regulators from other areas or disciplines continue to express concerns about the use of tracking technology and other aspects of online data collection and usage. They do so both generally but also specifically in relation to the way it may be impacting on children and young people. Technological convergence seems to be generating its own regulatory convergence as the interdependence of the different strands of activity becomes clearer.

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[xv]. 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 the European Commission 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 on its own and without more 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.

The emergence of pre-paid cards

There was a time when it was widely, if wrongly, thought that if an online vendor insisted on payment with a credit card e.g. using the Visa or Mastercard logos and payment mechanisms, this was the same as saying they would only deal with persons aged 18 or above.

Today this position is no longer tenable. A plethora of cards using the Mastercard, Visa, Maestro, Amex and other payments networks have become available. These cards are on sale in corner shops, petrol stations and many other retail outlets, large and small. Whilst some card issuers say they should only be sold to persons over the age of 18, that is not the case with all of them and anyway there is no law requiring this. Enforcement of that provision is thought to be, for all practical purposes, non-existent. However, leaving aside who the cards can properly be sold to or in fact are being sold to, some are sold and promoted for use "by persons of any age" whereas others seem to specify 13 as the minimum age.

Mastercard and Visa prefer to call these "stored value" cards. However, much to their annoyance the fact that they allow the use of the Visa and Mastercard logos means these bits of plastic are destined to be known for quite some time as "pre-paid credit cards".

Where the card is a re-loadable pre-paid card, there seems to be less scope for the card to be misused because it appears the transaction has to be tied to an existing bank account or credit card or to involve some other level of identification and authentication of the user. It is only the non-reloadable low value cards that in practice have few if any constraints or checks.

The non-reloadable cards can, in effect, be bought and used anonymously[xvi] . This is facilitating the purchase of goods and services online which children and young people could not normally make in shops in the real world because their appearance would betray them. Alternatively, because some

companies continue to accept a credit card number as proof that the holder is over 18, it is easing the entry of children into online environments from which they would otherwise be barred.

To some observers the current upper cash limits of these cards (150 Euros) may seem comparatively small, but for many purposes, including many criminal purposes e.g. buying child abuse images, counterfeit software, alcohol, tobacco and knives, the limits are quite substantial. It seems that the limits of these cards are going to be increased to 250 Euros and in some cases 500 Euros. It is hard to see how this can help online child safety. A consultation is currently under way in this area[xvii].

It is sincerely to be hoped that if any new rules emerge they will close down the possibility of using pre-paid credit cards anonymously on the internet or other remote environments.

Facilitating low value payments in the real world is one thing, rather like Oyster cards in London or Octopus cards in Hong Kong, but if the authorities blindly allow these technologies to translate into the online space they will, in effect, be opening the door to a potentially enormous increase in low value, low level crime. Law enforcement agencies will not thank them for this, and neither will anyone else.

Visa, Mastercard and the other card franchises are doing a lot to try to stamp out the improper use of their online payments facilities generally, but the fact that they have allowed these new types of pre-paid cards to emerge in the way that they have does rather run in the opposite direction and begs several questions.

Some of the pre-paid card issuers have taken steps to block their use on certain types of web sites e.g. sites which are specific to particular age restricted products or services such as gambling or alcohol, but not all of them have done this and many age restricted items are on sale through generic sites e.g. supermarket websites, where it seems such restrictions cannot be applied so easily.

The banks and financial institutions quite properly point out that, where the sale of an age restricted product or service arises, under the current law in most countries it is the retailer's responsibility to determine the age of the person doing the buying, in the online world as it is in the real world. There is no doubt that is true but one cannot help but feel some sympathy for the retailers as the financial institutions promoting these prepaid cards have certainly not made their job easier in respect of online sales.

It should not be possible for any method of payment to be used online to facilitate an illegal purchase of an age related product or service, but those pre-paid cards which can be bought for cash and used without any effective form of authentication of the user, seem almost to have been customised to facilitate illegal trade of one kind or another. It is the anonymity that opens the door to that.

The advantages of pre-paid cards are plain enough in terms of reaching out to the large number of people who cannot gain access to conventional credit or who do not want it for whatever reason. eNACSO has no locus or reason to object to the cards on principle. But the problems they have are creating should have been foreseen and avoided. They ought now to be addressed, either by their creators (the finance industry) or their business benefactors (retailers) who use them, or both.

---ooo---

Endnotes

[i] http://www.virtualworldsnews.com/2007/08/disney-acquires.html

[ii] http://www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf

[iii]http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf

[iv]IMRG/CapGemini Sales Index, September 2010, see http://www.imrg.org/8025741F0065E9B8/(httpPages)/FAE5B4EDA9020E448025744F0038D60B?OpenDocument

[v]"Consumer Kids", Ed Mayo & Agnes Nairn, Constable & Robinson Ltd, London 2009, at pages 5 and 18.

[vi] http://www.guardian.co.uk/news/datablog/2010/feb/23/cost-raising-child#data

[vii]http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html

[viii]See "Myths and Fallacies of "Personally Identifiable Information", Narayanan and Shmatikov, June, 2010, http://unescoprivadesa.urv.cat/media/_pdf/shmat_cacm10.pdf

[ix] Owners of web sites visited by children and young people also point out that many of the trackers being used are installed on children's and young people's computers by third parties, not directly by themselves, implying they have little or no responsibility for them and not all trackers collect or provide information that would be of interest to advertisers.

[x] http://www.youronlinechoices.com/wp-content/uploads/2010/07/IAB-UK-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf at section 3.

[xi] http://www.oft.gov.uk/OFTwork/consultations/closed-awaiting/eprotection/

[xii] http://www.oft.gov.uk/shared_oft/consultations/eprotection/oft1253

[xiii] Although see the discussion on the emergence of so-called "persistent cookies".

[xiv]http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

[xv] The Byron Review, 2008, page 20, para 1.21 -

[xvi] The fact that many outlets selling the cards deploy CCTV hardly counts as a complete rebuttable. -

[xvii] http://www.hm-treasury.gov.uk/8439.htm. -