March 2006

MARKETING: PART 3

Data protection and direct marketing: child's play

SLAUGHTER AND MAY

Rob Sumroy, Partner

The first article in this series "Introduction to data protection and direct marketing: the rules of the game" set out the legislative and regulatory framework that direct marketers are required to work within. The second article "Getting the right consent on data capture" went on to examine in greater detail the requirement to obtain consent prior to carrying out marketing activities, including the correct form of consent and the possible means for procuring consent. This third article considers the rules and guidance that apply in relation to direct marketing to children and, amongst other issues, the types of consent that are required.

The lucrative child market

According to new research from Halifax PLC, the average amount of pocket money children in Britain receive is £7.82 per week, creating collective yearly spending power of £70m. Such figures are a startling indication of the immense spending power wielded by children in Britain. The marketers have not been slow in picking up on this potentially lucrative market and, as corroborated by the increasing number of commercial children's websites, in recent years there has been a dramatic increase in, and intensification of, exposure of children to commercially sponsored media. This article considers the regulation of such exposure.

Exploitation of a vulnerable class

Taking into account levels of trust, credulity and lack of maturity, children, in the context of data protection and direct marketing, must be viewed as a vulnerable class of people. The majority of children are unlikely to possess sufficient maturity, experience and knowledge to be able to appreciate the significance of personal data and are therefore less likely than adults to refrain from disclosing such data when it is requested by direct marketers. It is unlikely that a child would appreciate the risks that disclosure of personal data could create.

The major concerns aroused by the disclosure of personal data to strangers by children include:

> the threat of child abuse;

> the potential for direct marketers to exploit a vulnerable class of people; and

> the disclosure by children of personal data relating to other people, for example their families, and the exploitation of such personal data for direct marketing purposes.

This article focuses on the issues in relation to direct marketing to children.

Fair and lawful processing

As the previous articles have explained, when providing direct marketing, the data controller is required by the first of the eight data protection principles, the fair and lawful processing principle, as set out in the Data Protection Act 1998 ("**DPA**") to comply with at least one of the conditions set out in Schedule 2 of the DPA, such as obtaining the data subject's consent. Neither the DPA nor the Data Protection Directive 95/46/EC (the "**Directive**") contain any specific provisions for children in this regard.

Considerations

The lack of a statutory framework setting out the rules as they should be applied to children creates a glut of uncertainty and raises several questions:

> Is parental consent required when obtaining and using children's personal data for direct marketing purposes?

> Should there be an age restriction below which children are not permitted to disclose personal data without parental consent?

> How can data controllers verify that the children they are dealing with are either above a certain age or have genuine parental consent?

> Can children disclose data relating to third parties?

> Can direct marketers entice children to disclose their personal data with the promise of prizes or the opportunity to play games?

> Can children's personal data be transferred to third parties?

> Can children's personal data be published on the internet?

> How should direct marketers inform children (or their parents) that they intend to use the personal data for marketing purposes?

Guidance

Bearing in mind the potentially serious consequences of personal data being disclosed by children, it is somewhat surprising that neither the DPA nor the Directive contain any specific provisions on data collection from, and marketing to, children. However, despite the lack of clarity provided by the statutory provisions, there is some guidance on the issue from the Information Commissioner as well as certain self-regulatory codes which help to address the wider consumer issues.

The Information Commissioner's Guidance

In 2001, the Information Commissioner provided guidance on this issue in relation to the internet only. This guidance can be found in section 11 of "Compliance Advice – Website Frequently Asked Questions" (which can be found on the Information Commissioner's website: www.ico.gov.uk) (the "**IC Guidance**"). The IC Guidance has not been expanded or updated and it would appear that the Office of the Information Commissioner has no plans to do so in the immediate future.

Advertising Code

The British Code of Advertising, Sales Promotion and Direct Marketing (created by the Committee of Advertising Practice and administered by the Advertising Standards Authority, the "**ASA**"), sets out rules which apply to non-broadcast marketing (the "**CAP Code**"). All UK organisations carrying out direct marketing must comply with the self-regulating regime. Section 47 of the CAP Code deals specifically with children. The CAP Code regards a "child" as someone under 16.

TrustUK

TrustUK is a non-profit organisation designed to enable consumers to buy online with confidence. TrustUK accredits associations and organisations that use codes of practice that incorporate certain core principles, the accreditation criteria. The four major codes that have currently been approved are owned by the Association of British Travel Agents Ltd ("**ABTA**"), the Direct Marketing Association ("**DMA**"); SafeBuy; and WebTraderUK.

The DMA code of practice sets standards of ethical conduct and best practice for direct marketers, and is administered and monitored by the independent DMA. All the new marketing and media channels, such as e-mail and SMS marketing, together with field marketing and door-to-door, are now included within the DMA code of practice, as well as the traditional media like direct mail, press and telemarketing. The general rules in relation to minors are found at sections 8.11-23, and section 19.25 contains specific rules relating to marketing to children online. The DMA code of

practice defines both "minors" and "children" as those less than 18 years unless otherwise stated. The DMA code of practice is unsurprisingly the most relevant of the codes when considering direct marketing to children, however the other codes do have limited references in this area that will be highlighted in this article.

Mobile Marketing Association

The Mobile Marketing Association ("**MMA**") produced, in November 2005, a code for responsible mobile marketing (the "**MMA Code**"). 'Mobile marketing' is any form of marketing, advertising or sales promotion activity aimed at consumers and conducted over a mobile channel. Methods of communicating for this type of marketing include voice files, SMS, MMS, WAP messaging, Java, SyncML and video and audio messaging. The MMA Code intends to set a benchmark of best practice for member marketers using the mobile medium. Section 5 considers how marketing to children should be regulated.

Parental Consent

European data protection legislation does not provide an obvious requirement for data controllers to obtain parental consent when dealing with children's personal data. The official guidance in the area suggests that when considering the necessity for parental consent a balancing act should be performed between the interests of the child and those of the data controller.

The Information Commissioner advises that, where a child is asked to provide personal data, unless it is reasonable to believe that the child clearly understands what is involved and is capable of making an informed decision, the consent of a parent or guardian is necessary.

The MMA Code requires parental consent to varying degrees depending on the age of the child in question and the activity, i.e. either collection of details, use of details, or the making of the details available to third parties. CAP produced, in May 2004, a help note on mobile marketing but this is far briefer than the guidance provided by the MMA, only requiring (i) verifiable and explicit parental consent before communicating via mobile with children, and (ii) a statement to be provided to the children at the point that personal data is requested informing them that parental consent must be given.

Fixed Age Requirement

In other areas of law, a fixed age is set at which young persons attain legal capacity. For example, ages have been fixed from which a person can purchase alcohol or cigarettes, get married, consent to medical treatment, or learn to drive etc. By contrast, the DPA does not set a fixed age at which a child may provide consent to the disclosure of personal data on his or her own behalf.

The IC Guidance comments on the absence in the DPA of such a fixed age. The Information Commissioner does not consider it valid to try to provide one, because such ability will depend upon the capacity of each child in question. As a general rule the Information Commissioner considers the standard adopted by TrustUK (www.trustuk.org.uk) in its accreditation criteria to be a reasonable one. This is that:

'Personal data must only be collected from children with the explicit and verifiable consent of the child's parent/guardian unless that child is aged 12 years or over, the information collected is restricted to that necessary to enable the child to be sent further but limited online communications and it is clear that the child understands what is involved'.

The above standard is based on the definition of a "child" as a person aged 16 years or under.

The CAP Code does not provide a fixed age either. It recognises that the way in which children perceive and react to marketing communications is influenced by their age, experience and the context in which the message is delivered. The ASA is said to take all of these factors into consideration when assessing marketing communications.

The DMA code of practice considers separately the requirement of parental consent for the collection of data in an online and an offline environment. When collecting data online, the members of the DMA must secure consent from all minors under the age of 16 whereas, if the data is collected offline, parental consent is only required for minors under the age of 14.

The DMA code of practice gives several specific examples of the application of the age restriction in relation to online marketing. Websites that are directed to children must not collect personal data from children under the age of 16 without first obtaining a parent or guardian's verifiable and explicit consent. Websites should ask children their age and if they are under 16 the child should be excluded from giving further personal information until they have obtained the verifiable and explicit consent of a parent or guardian. Orders for goods or services should not be accepted from children under 16 without first obtaining a parent or guardian's verifiable and explicit consent. This requirement is also found in the WebTraderUK Code. The DMA code of practice emphasises throughout this section that contracts are legally unenforceable against minors.

The DMA code of practice is accompanied by non-binding best practice guidelines. Section 3.1.6 of the Email Marketing Council Best Practice Guidelines dated 27 July 2004 considers e-mail marketing to children. Given the general air of mistrust amongst the general public, the DMA has decided that, under best practice guidelines, no person under the age of 16 should be the target of an email marketing campaign. The DMA accept the difficulties with this, in that, there is no way to guarantee the age of any child who signs up for email marketing.

The MMA Code is different in that it provides age ranges (under 12, 12-13, 14-16, and 17) with different rules for the collection of details, the use of the details, and making the details available to third parties for each band. The rules are more stringent for the younger age brackets, for example no personal data may be collected from children under 12 without explicit and verifiable parental consent but direct marketers may collect such personal details from children of 17 years that the marketers need for the purpose of marketing to them without the need for parental consent.

It is clear that children mature at different ages and a fixed age is, to an extent, arbitrary. However, it may be argued that the flexible rule currently preferred causes problems to businesses as, for example, website operators have no means to ascertain in each individual case whether a child understands what is involved. The flexible rule could potentially undermine the protection of younger children as website operators may have difficulty complying with such a vague rule and could defy the law. A fixed age would provide legal certainty to website operators but if an age restriction were to be introduced, extensive research into the awareness and understanding of children of data protection issues and their actual internet viewing habits should be undertaken in order to set the age at an appropriate level.

Verification

There is a significant problem with having a fixed age at which a child can be deemed, in terms of data protection, to be able to act in his or her own right, and below which parental consent is required when requesting personal data from children below that age: the problem being the technical difficulties, especially in an online context, involved in the verification of such ages and consents.

There are various methods of attempting to verify parental consent, but many of the current methods are flawed in terms of either being administratively unworkable or they are unreliable for accurate verification of genuine consent.

One of the easier verification tests for a child to sidestep is the requirement of some websites for the child to tick a box to confirm that they have parental consent. This can be satisfied by a simple lie. Other methods include: requiring the child to provide a parent's email address for the data controller to send an email to that address requesting consent; requiring a consent form to be signed and faxed; accepting and verifying a credit card; having trained staff take a call from parents; requiring parents to send an email with a digital signature; and requiring a PIN number or password to be provided. Even credit cards may not actually genuinely verify that it is the parent giving the consent and third party authentication services including the use of digital signatures are not in common use.

The problems with verifying consent are addressed by the IC Guidance. The Information Commissioner states that it will not usually be sufficient to simply ask children to confirm that their parents have agreed by means of a mouse click. It will in all likelihood be necessary to revert to postal communication. Requiring postal consent is a safe verification method but is time consuming (i.e. the time taken for the letter to be received by the website operator) and difficult to administer.

All of the more effective methods of verifying parental consent place a hefty compliance burden on data controllers, for example the requirement to have trained telephone operators taking calls from parents, and consequently some

data controllers may choose not to comply. The Information Commissioner states that if parental consent is the required standard but the website operator concludes that the effort in verifying the consent is disproportionate, the proposed marketing activity or other course of action should not be pursued.

The DMA code of practice requires that parental consent be "explicit and verifiable" but does not specify how this consent should be verified.

The problems in acquiring genuine verified parental consent are not easily overcome. It is possible that the use of third party authentication will become more commonplace but for the meantime it is for the data controllers to use the slow, difficult to administer and often unreliable methods currently available or to desist from obtaining children's personal data.

Personal Data Relating to Other People

As mentioned above, a major concern about the disclosure of personal data to direct marketers by children is the potential for children to disclose personal data about other people who would not have given their own consent, for example members of a child's family. The Information Commissioner's advice on this is issue is that this practice is likely to breach the requirements of the DPA.

The DMA code of practice also clearly states that, with regard to online marketing to children, personal information relating to other people, for example a child's parents, must not be collected from children.

Enticements

The Information Commissioner is clear that enticing children to divulge personal data with the prospect of a game, prize or similar inducement is likely to breach the requirements of the DPA.

The DMA code of practice prohibits advertisers from making a child's access to a website contingent on the collection of personal data. Nor may advertisers entice a child to divulge personal information with the prospect of a special prize or other offer.

Transfer of Personal Data to Third Parties

The Information Commissioner applies a flexible rule in the case of the sale of lists of personal data containing information collected from children. He considers that if personal data collected from children are to be disclosed or transferred to third parties this should not take place without the explicit and verifiable consent of the child's parent or guardian unless it can be demonstrated that the child really appreciates what is proposed and the consequences of his or her actions.

Publication of Children's Personal Data on the Internet

Often website operators facilitate the publication of personal data relating to children on the internet. This can occur in a variety of arenas, for example, chat rooms, instant messaging services and message boards. These facilities can be used for marketing purposes, for example chat rooms can be themed around certain products such as children's films or even toys. The Information Commissioner considers that where a website operator wishes to publish personal data relating to a child on the internet the verifiable consent of the child's parent or guardian should usually be obtained. Whether it is necessary to seek the parent or guardian's consent to publication, rather than that of the child, will again depend on the circumstances, in particular the age of the child, and whether or not the data controller can be certain that the child fully understands the implications of making their information available on the internet.

The DMA code of practice states that websites are not to post or disclose children under the age of 16's personal data without first obtaining a parent or guardian's verifiable and explicit consent. It goes on to say that where a website offers children interactive activities such as chat rooms, information by which the parent can understand the nature of these activities and the consequences of a child's participation must be made available in a privacy policy statement.

Privacy Notices

Direct marketers are required by the DPA to explain to data subjects that they intend to use their personal data for marketing purposes.

The IC Guidance states that "website operators should recognise that children generally have a lower level of understanding than adults and notices explaining the way their data will be used should be appropriate to this level of understanding and should not attempt to exploit any lack of understanding".

The DMA code of practice contains a similar provision. If collecting children's personal information, the website operator must post a privacy policy statement. This statement must be able to be understood by a child audience, posted in a prominent place, for example on the home page and where the information is collected, and must contain the following: a statement that data will not be collected online without the verifiable and explicit consent of a parent or guardian; a statement that the provision of requested information is entirely voluntary; an explanation that a parent can acquire access to the information collected from the child; and where the website offers children interactive activities such as chat rooms, information by which the parent can understand the nature of these activities and the consequences of a child's participation. The DMA code of practice also requires, at the point where the personal information is requested, a notice to be provided informing children of the requirement to obtain parental consent (in easily understood language) including an explanation of the purposes of the data, i.e. marketing.

General Requirements

The general rules in relation to marketing communications and minors at sections 8.11-23 in the DMA code of practice are extremely similar to those in the CAP Code, to the extent that the same wording is used for several provisions. These requirements focus on the content of the marketing communications, for example, they should contain nothing that is likely to result in the physical, mental or moral harm of children nor should they exploit their credulity, loyalty, vulnerability or lack of experience.

Comment

It will be apparent from this article that the law and guidance in this area may be seen as, at best, a complex web of differing advice and, at worst, inconsistent and confusing to the extent that data controllers may decide to simply ignore their responsibilities. The challenge for the legislators is to produce a set of clear rules and guidance that provide sound protection for vulnerable children, are easy to understand and, consequently, encourage compliance.

The next and final article in this series will consider the data protection implications of transactions involving the sharing or transfer of personal data in a database in a marketing context; in particular, if consent to the transfer/sharing is required and the practical implications for both the seller and the purchaser of the database.

Executive Summary

The Law and Guidance

The law in this area is unclear to the extent that neither the DPA nor the Directive contain any specific provisions relating to children. There is, however, guidance in the area provided by the Information Commissioner. This guidance is extremely brief and is limited in its scope to the internet and the issues relating to websites and it is unclear how applicable the guidance is to other forms of direct marketing to children.

The IC Guidance is supplemented by certain self-regulating codes. These codes provide a useful guide as to what is appropriate but they cannot be entirely relied upon because not all data controllers are members of trade organisations such as the DMA and there is inconsistency between the codes, for example as between the DMA and the MMA regarding age requirements.

Parental Consent

The Information Commissioner suggests that when considering the necessity for parental consent a balancing act should be performed between the interests of the child and those of the data controller. The MMA, however, does not advocate such a flexible rule and instead provides requirements for parental consent for different activities depending on the age of the child in question.

Fixed Age

There is no legal minimum age at which a child can make his or her own decisions regarding the disclosure of their personal data. The Information Commissioner has advised that it would be invalid to implement such an age restriction and that the capacity of each individual child should be considered. Other guidance however does provide fixed ages, ranging between 12 and 18, at which children may disclose their personal data without parental consent.

Verification

There are several potential methods of verifying a child's age or genuine parental consent. However, the methods tend to either be administratively difficult to perform or are not sufficiently accurate. As modern technology advances these problems are likely to disappear but for the time being there is no commonly used fool proof method. The Information Commissioner's stance is that if parental consent is required but the verification obligation is deemed by direct marketers to be overly burdensome the activity should not be allowed to take place.

Personal Data Relating to Other People and Use of Enticements

The guidance is consistently clear that these activities are not permitted.

Transfer of Personal Data to Third Parties

If personal data collected from children are to be disclosed or transferred to third parties this should not take place without the explicit and verifiable consent of the child's parent or guardian unless it can be demonstrated that the child really appreciates what is going on and the consequences of his or her actions.

Publication of Children's Personal Data on the Internet

The DMA code of practice requires parental consent from children under the age of 16 whereas the Information Commissioner applies the flexible rule and requires the capacity of the individual child to be taken into account.

Privacy Notices

Direct marketers are required by the DPA to explain to data subjects that they intend to use their personal data for marketing purposes. When dealing with children, it is recommended that this information is provided to the children in a manner that will be easily understandable to them.

A version of this article appeared in Volume 6, issue 4 of Privacy and Data Protection (March 2006)

London
One Bunhill Row
London EC1Y 8YY
United Kingdom
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Paris
130 rue du Faubourg Saint-Honoré
75008 Paris
France
T +33 (0)1 44 05 60 00
F +33 (0)1 44 05 60 60

Brussels
Square de Meeûs 40
1000 Brussels
Belgium
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
47th Floor
Jardine House
One Connaught Place
Central
Hong Kong
T +852 2521 0551
F +852 2845 2125

Published to provide general information and not as legal advice © Slaughter and May, 2006