Agnes Nairn

was a market research practitioner for many years before becoming an academic researcher and writer. She is based in the UK but is affiliate Marketing Professor at EM Lyon Business School and Visiting Marketing Professor at RSM Erasmus University in the Netherlands. Her research focuses on issues relating to children's marketing and she has published in a wide range of international journals.

Dowsiri Monkgor

worked on this research as part of her Masters in Management thesis at the University of Bath. Having successfully completed this, she is now studying for a Masters degree in Organisational and Social Psychology at LSE.

Keywords: children, privacy, data protection, online, parents, control

Agnes Nairn
U.P.R. Marchés et Innovation
EM Lyon Business School
23 Avenue Guy de Collongue
69132 ECULLY
France
Tel: +44 7796 585449
E-mail: Nairn@EM-Lyon.com

Papers

Children and privacy online

Agnes Nairn and Dowsiri Monkgor

Received: 15 January 2007

Abstract

Kids are spending *more money* on goods and services and *more time* online than ever before. This makes them an incredibly tempting target for online marketing. But what are the data protection issues where children are concerned? This paper considers child data protection using the concepts of knowledge, control and parental involvement; it reminds us of the DMA code of practice for online marketing to children and presents review of how 20 of the top children's websites match up to the code. While most of the children's websites do post a data protection policy, it is not easy for children to find or understand; few policies are displayed at the point of information collection; children have little control over what happens to any information they do disclose and the common practice of involving parents is woefully inadequate. It is hoped that this paper will highlight some of the issues involved in protecting children's online privacy and encourage debate on how the industry should proceed in this tricky area.

Journal of Direct, Data and Digital Marketing Practice (2007) **8**, 294–308.
doi:10.1057/palgrave.dddmp.4350063

Background

Children's purchasing power has tripled since the 1990s. The children's market in the UK alone is now estimated at £3bn for purchases made with children's own money and £30bn when child-influenced purchases are included.¹ Globally, children have been estimated to spend an annual \$300bn² of their own money and influence a further \$1.88bn of family spending.³ And as family styles democratise, children's say in household purchase decisions seems set to increase.⁴ Children are particularly influential in the purchase of technology products where they often have more sophisticated technical knowledge than their parents,⁵ being less risk averse when faced with novelty.⁶ Children, thus, now constitute a large, attractive and profitable direct and indirect market for global corporations.

It seems that the most effective way to tap into this market is by the internet. Online advertising in the UK is growing at about 40 per cent a year and, according to media buying agencies, represented 14 per cent of overall UK ad spending last year.⁷ That is the highest level in the world, and more than double the percentage in the United States. Almost all homes in the UK now have a computer as well as a

Children's internet usage is growing rapidly

television with 70 per cent of children now having home internet access. While the hours in front of the television screen are decreasing very slightly, children's internet usage is growing rapidly with 5–16-year-olds now spending 1.8 h a day online. And with 40 per cent having a PC of their own, children's online experiences are becoming increasingly less supervised by adults.¹

This paper tackles the question of how the industry can ensure that children's privacy is protected in this fast-moving online environment.

Definitions of privacy

Defining privacy

In 1890, Warren and Brandeis⁸ first defined privacy in the *Harvard Law Review* as 'the right to be let alone'. Almost 80 years later, Westin^{9,10} highlighted a concern with 'Privacy in Computer Society' and introduced the notion of an individual having rights and control over personal information collected by a third party. In 1978, Wasserstrom¹¹ urged governments to consider 'the question of the kind and degree of control that a person ought to be able to exercise in respect to knowledge or the disclosure of information about himself or herself' (p. 148). As the ensuing quarter of a century has witnessed an unprecedented evolution of data collection technologies, privacy and data protection have remained a hot topic. It is now widely acknowledged that we live in a 'Surveillance Society',¹² and for some this simply means that our rights to privacy have thus effectively disappeared. For example, in 1999, Scott McNealy,¹³ the chief executive officer of Sun Microsystems, claimed, 'You already have zero privacy. Get over it'. Most citizens and corporations have, however, not abandoned the ideal of maintaining forms of data protection, and as children enter the marketplace in force, it is imperative that the issue remains at the forefront of social debate. Indeed, many writers in the field continue to make efforts to refine the definition of privacy in a contemporary context. A review of the past ten years of such literature shows that definitions of online privacy have now converged on two central concepts: control and knowledge.^{14–19} A very brief overview is provided below.

Consumers' control over their own privacy

Control

Goodwin's¹⁴ influential paper of the early 1990s builds on the core ideas of Westin⁹ who was the first to suggest that consumers might be able to control their own privacy by exercising intellectual property rights over the collection and usage of personal information. He adds a contemporary dimension to Warren and Brandeis'⁸ original notion of the right to be let alone by proposing that consumers should also have control over unwanted intrusions, which might now include techniques such as spam, pop-ups, pop-unders and interactive banners. Foxman and Kilcoyne¹⁵ have made a useful contribution to the application of control by operationalising it specifically in a marketing context. Their research shows that consumers believe strongly in ownership rights to their personal information. Foxman and Kilcoyne¹⁵ claim that marketers, therefore, have a duty to inform customers that data are being collected and the uses to which they will be put; that customers should have

access to that data in order to amend errors and also that customers should have choices about disclosure, particularly to third parties.

Knowledge

Consumer unable to exercise control in the absence of knowledge

A number of commentators have noted, however, that the consumer is unable to exercise control in the absence of knowledge. Foxman and Kilcoyne¹⁵ (p. 107), for example, state that 'we distinguish privacy states operationally on the basis of who controls consumer data and whether or not consumers are informed about data collection and privacy rights'. Indeed, as Awad and Krishnan¹⁹ point out, knowledge is a determinant of perceived control.^{20–22} A consumer is not truly in control if s/he is not in possession of facts and choice options. This highlights not only the rights of consumers to control their data but also to be informed about what data are being collected; the purposes to which they are being put and what choices the consumers have to withhold information.

2x2 frameworks

This dual definition of privacy has led to a number of authors proposing 2x2 frameworks to diagnose, identify and analyse states of privacy.^{23,15} Four possibilities are offered: consumers are aware of their rights and have control over them; consumers are aware of their rights but, in practice, are not able to opt in or out of data collection; consumers are not aware of their rights although, in fact, choices about disclosure are available and consumers have neither knowledge of choices nor the ability to exercise them. Clearly, from a data protection point of view, the most desirable position for an online marketer to adopt is one where customers have both full knowledge and awareness of the details of information collection and have a clear choice about what is collected, when and for what purpose. Moreover, research suggests that when consumers perceive themselves to be fully informed and in control, they are more likely to wish to form an ongoing trusting relationship with the organisation requesting such information.²⁴ Thus, there is both a socially responsible normative case and a pragmatic business case²⁵ to be made for basing our understanding of privacy rights on the tenets of knowledge and control.

But can we use the same constructs when considering children's data protection and privacy? Are children's rights different from adult rights? Do children have the same abilities as adults to understand and control the process of information collection?

Conceptualising children's online privacy

Children's rights

Most countries in the world are signatories to the United Nations Convention on the Rights of the Child, which was first adopted in 1980. This charter is thus the usual point of departure for any form of legislation or best practice guidelines relating to children. The scope of children's rights is, however, broad, and the definitions occasionally conflicting. David Archard, the author of the influential book, 'Children: Rights and Childhood',²⁶ notes that the Convention distinguishes between two quite different views of children's rights. On the one hand, it proposes the child's right to 'protection', and on the other hand the child's right to 'participation'. Protection rights rest on a

Tension between conceptualisations

conceptualisation of the child as helpless and defenceless in the face of potential dangers, while participation rights are based on a view of children as active, autonomous agents. Archard illustrates the tension between these conceptualisations by showing that two key Articles of the Convention are based on different interpretations of children's rights. 'Article 3 enjoins every agency dealing with children to make their best interests its primary consideration; Article 12 accords to all children, capable of doing so, a right to express their views on any matter affecting them, these views being given a weight proportionate to their age and maturity' (Archard,²⁷p. 7). If the world's core contemporary charter on children's rights contains these ambiguities of definition, it is clear that today's societies are far from agreeing upon how children's interests are best served.

Yet, navigating this tension between the active and passive view of the child is paramount in deciding if or how the notions of knowledge and control should be applied to children's online privacy. Should online data collection from children simply be banned in order to protect them from possible unwanted consequences, or should children be accorded the right to control the uses of their personal information as they see fit? And if children are to have some form of control, how can it be ensured that children of different 'ages and maturity' truly have enough awareness and knowledge of the alternatives to exercise control? The next section considers how these questions have been addressed in the current regulation for children's online data protection.

No legislation in the UK dealing with online marketing to children

Legislation and codes of practice

In the UK there is no set legislation that deals with online marketing to children. This contrasts with the situation in the USA where The Children's Online Privacy Protection Act (COPPA, 1999; 112 Stat. 2681) specifically prohibits the online collection, use and disclosure of personal details of children under 13 without parental consent.²⁸ Specifically it requires operators of websites targeting children under 13 to:

- (1) post prominent links on their sites to notices outlining the collection, use and/or disclosure practices involving personal information
- (2) notify parents about collection practices and obtain their consent before information collection, use and/or disclosure
- (3) cease the practice of linking children's participation in online activities to the collection of additional personal information
- (4) allow parents the opportunity to review information on their children, delete this information from databases if desired and prohibit further collection of information
- (5) formulate procedures to protect the confidentiality, security and integrity of personal information.

Knowledge and control

It is clear that this legislation rests on the concepts of knowledge and control. In terms of knowledge, this Act requires that children need to be made aware of privacy policies. In terms of control, it outlaws the

Definition of a child is confused

practice of making data disclosure a prerequisite to participating in a desirable activity, which would effectively compromise the child's control. The provisions within COPPA also address the tension between the child's right to protection and also right to empowerment. This is done, quite simply, by including parents in the process. Parents must be notified about information collection practices and their consent obtained prior to data collection; and they must have the opportunity to see, alter and withhold information on their children. In effect, the legislation places the parent as an intermediary between the website owner and the child, with the parent having final responsibility for defining the child's rights. This appears a reasonable response to a difficult question.

This legislation does not, however, apply outside the USA and those marketing to children online in the UK must base their decisions about appropriate conduct on a mix-and-match selection from an assortment of self-regulatory codes and best practice guidelines. This is not necessarily a straightforward matter. At the most fundamental level, the existing guidelines do not agree on the definition of a child. The Children and Young Person's Act defines a 'minor' as under 14 and a 'young person' as aged 14–18; The Advertising Standards Association's (ASA) Code on Advertising Practice (CAP) considers a child as anyone under 16; and Ofcom regard a 'child' as under 15 and a 'young person' as between 16 and 17. The Information Commissioner — who is responsible for regulating UK data protection — takes the view that children over 12 are capable of giving their consent to their details being collected by third parties.

Probably the most comprehensive and rigorous guidelines are provided by the DMA Code of Practice, which was updated in 2006 to specifically include OnLine Marketing to Children (Sections 19.25–19.34). The sections relevant to privacy are shown in Table 1.

This is a comprehensive Code that has many similarities to COPPA as it rests on the three principles of knowledge, control and parental involvement.

Knowledge

It requires the operators of sites aimed at under 18s to make users aware of the purpose and scope of data collection activities and to ensure that such information is displayed in a prominent position and in language which can be understood by children (19.31, 19.34).

Control

It requires site operators not to compromise children's control by making the divulgence of personal information a prerequisite to participate in a desirable activity (19.32) and it requires sites to explain how consent for data collection by advertisers can be given.

Parental involvement

It requires that children give their age before any other information is collected and that if they are not 16 that no more information is

Table 1: DMA code of practice: online marketing to children

19.25	Children for this purpose are those under 18 years of age unless a different age is mentioned. Reference to parents includes, where applicable, legal guardians.
19.28	Websites that are directed to children must not collect personal data from children under 16 years of age without first obtaining a parent/guardian's verifiable and explicit consent.
19.29	Websites that are directed to children and that collect personal data from children must not publicly post or disclose personal data collected from children under 16 years of age without first obtaining a parent/guardian's explicit consent.
19.30	Websites that are directed to children and that collect personal data from children must require a child to give their age before any other personal information is requested. If the age given is under 16 the children should be excluded from giving further personal information until the appropriate verifiable and explicit consent has been given.
19.31	A notice informing children of the requirement for parental or guardian's consent must be shown at the point where personal information is requested. This notice should be clear and prominent and written in language that will be easily understood by young children. It should include an explanation of the purposes for which data are being collected that is for marketing purposes and how that consent may be given to the advertiser.
19.32	Advertisers must not make a child's access to a website contingent on the collection of personal information or entice a child to divulge personal information with the prospect of a special prize or other offer.
19.33	Personal information relating to other people (for example parents) must not be collected from children.
19.34	Members collecting personal information from children must post a privacy policy statement on their internet website (or for other means of online communication where this may not be practical, they must provide a prominent link to where this information can be accessed). Such a statement, and any link to it, must be understandable by a child audience and posted in a prominent location – both on a site's home page and any page where information is collected. In addition to the requirements set out in para 19.22, such a statement must contain: <ul style="list-style-type: none"> (a) a statement that data will not be collected online without the explicit and verifiable consent of the parent/guardian (b) a statement that provision of the requested information is entirely voluntary (c) an explanation of the measures by which the parent/guardian may exercise their right to have ready and inexpensive access to the data held regarding the child in their care, so as to contest inaccurate or incomplete data, verify the information and correct it as appropriate (d) where a website offers children interactive activities such as chat, message boards, free email services, posting of home pages etc information by which the parent/guardian can assess and understand the nature of these activities and the consequences of the child's participation.

collected before 'verifiable and explicit' parental consent is obtained (19.30). It requires parental permission for all data collection from under 16s (19.28) and all disclosure of personal data from under 16s (19.29). It also requires that children are informed that parental consent must be obtained and that this information is posted in a prominent place and in easy to understand language (19.31, 19.34).

Current best practice

Like COPPA the tension between whether children have the right to control their own personal information or the right to be protected from those collecting the information is resolved by requiring website

owners to involve parents in the child privacy process. Given the consensus between these two sets of guidelines, it is probably safe to say that together they constitute current best practice.

But given that only members of the DMA are bound by this Code in the UK, how well is children's online privacy really protected? Are companies marketing to children working within best practice? And are these notions of best practice actually effective in reality? The next section contains a review of the data protection provision offered by the websites which are most visited by UK children aged 9–13.

The research

20 most visited sites

A list of the 20 most visited sites was compiled as part of a survey completed by 557 children aged 9–13 from six very different schools in the South West of England and South Wales in Spring 2006. This age group was chosen as children below 8 are not very heavy internet users, while the 9–13-year-olds fall within most classifications of 'children' by regulatory bodies. Children completing the survey were asked to list the sites they often visited, and a simple count was made across all respondents. For the purposes of this paper, search engines such as Google and Yahoo have been taken out of the list as have noncommercial sites such as the BBC sites. Given the fast evolution of sites, this top 20 could well have changed in the months since the survey was completed, but such is the nature of research on the internet. It is also possible that children in other parts of the country may have listed different sites. Research from ChildWise,¹ however, indicates that the viewing habits of our sample is not significantly different from the national population as a whole, and we are thus satisfied that these sites are accessed by very large numbers of children across the UK. The top 20 sites are shown in Table 2.

Four areas addressed

The research took the form of a 'structured observation' of the sites. The questions used to guide the observation are shown in Appendix A and relate to the best practice principles circumscribed by COPPA and the DMA Code. Four areas were addressed: Nature of Data Collected, Knowledge (Does the site make children aware of data protection issues?), Control (Does the site enable children to control what and how personal data is used?) and Parental Involvement (Does the site require parental permission for data collection?). Key findings from each of these areas are reported below.

Nature of data collected

Eighty-five per cent of the 20 sites collected personal information from children. Only three sites visited did not collect any data. E-mail address and name were the most common types of information collected with other information including address, postcode, city, country, date of birth, gender and age (Figure 1).

Most information disclosure was 'compulsory' in that the child could not fully participate in the site activities without divulging some personal details. Fifteen per cent of the sites collected information as a

Table 2: Top 20 sites for children aged 9–13

www.miniclip.com
www.freewebs.com
www.teagames.com
www.disney.co.uk
www.piczo.com
www.freeonlinegames.com
www.habbohotel.co.uk
www.myscene.com
www.cartoonnetwork.com
www.nick.co.uk
www.neopets.com
www.diddl.com
www.albinoblacksheep.com
www.streaming-clips.com
www.puffgames.com
www.cheatplanet.gamesradar.com
www.newgrounds.com
www.popcap.com
www.mousebreaker.com
www.dressupgames.com

Figure 1: Type of information collected by the websites

prerequisite to using the site at all, while 35 per cent required information in order for the child to participate in desirable activities such as receiving newsletters, sending game reviews, downloading fun things, for instance, screensavers, wallpaper or ringtones, taking part in games and quizzes, putting postings on message boards or forums, asking the webmasters questions or sending clips to friends. A further 35 per cent required information for the personalisation of a site. Thus, the practice of the vast majority of popular sites for UK 9–13-year-olds does not correspond to the spirit of the DMA code or of COPPA that data collection from children should be voluntary and that children should not be enticed to divulge information with the prospect of a reward, such as participating in desirable activities.

Awareness of privacy options

Knowledge: Making children aware of privacy options

According to paragraph 19.34 of the DMA code, website operators should post a privacy policy statement 'in a prominent location — both on the site's home page and any page where information is collected'. Ninety per cent of the sites did post a privacy policy on their site (the two exceptions being streamingclips.com and puffgames.com). Almost three quarters of the sites (71 per cent), however, did not give privacy information at the point of information collection. This means that in order to obtain information about privacy policies, children had to actively seek them out. Eight-five per cent of the sites did have their privacy policies on the home page, but this information was not always easy to find. One of the most popular sites, www.miniclip.com, posted its privacy policy one click away from the front page under 'terms and conditions' (see Figure 2).

Figure 2: Privacy policy hard to find

Even where a privacy policy was posted on the front page, it was often at the bottom of the page in small writing which was the same colour as the rest of the text. Arguably, this is not prominent enough to genuinely give children the knowledge they need about privacy. The Nickelodeon home page shown in Figure 3 is an example of a privacy policy that is not in a prominent location. The writing is small, the same colour and font as the surrounding text, and the child must scroll down to see it.

Some sites, however, do position their privacy policies at the top of the page or use a bold font or highlighted colour. An example from www.cartoonnetwork.com is shown in Figure 4.

Paragraph 19.31 of the DMA Code states that a privacy notice should include an explanation of the purposes of data collection. All sites with a privacy policy explained what is done with the information and 94 per cent explained why. All policies included some details about data sharing with third parties. The language used in these policies, however, was rarely understandable to children; the text was very long and the script tiny. An exception is www.popcap.com which, ironically, claims to be a site for over 18s only (Figure 5).

Overall, commercial organisations are not making it easy for children to gain knowledge about privacy issues on their sites. While most have privacy policies they are hard to find, and when they are found they are hard to decipher. Perhaps most importantly the information on privacy is not available at the point where the child is actually disclosing personal data and is not written in a form accessible to children.

Commercial organisations do not make it easy for children to gain knowledge about privacy issues on their sites

Control

We have seen that knowledge is a prerequisite of control. As knowledge provision is very poor on the top children's sites, it follows that children also have limited control over their data. Their control is

Figure 3: Privacy information not prominently displayed on home page

Figure 4: Privacy policy displayed more prominently

Figure 5: Privacy policy written in language understandable by children

further compromised by the fact that on most sites children cannot have full access to all activities if they do not give some information. This limits the control they have over disclosure and does not correspond to the spirit of the DMA code paragraph 19.32. Within some of the privacy policies themselves, children were offered a certain amount of control. Seventy-six per cent of the sites explained what choices site visitors had in terms of how their information was used; 59 per cent explained if and how visitors could access, update or correct information held about them; 53 per cent explained if and how visitors could delete their information; and 94 per cent gave a contact address

Information about data privacy is available but difficult to find

for privacy queries. Eighty-two per cent of the sites provided the option of opting-out of their mailing list. Only 45 per cent, however, offered opt-outs from third parties' lists and only 35 per cent offered opt-outs from affiliates' lists. This does not offer much control to the child over where the information may ultimately be going. Moreover, only 59 per cent of the sites which collected information provided the opt-out choices on the same page or next screen, and on 35 per cent of the sites the children had to go to the privacy policy page to find out about opt-out choices. All the sites that had privacy policies explained that cookies from other sites might be used, but there was no option to opt-out of the use of cookies. Interestingly, cookies and other forms of spyware are not specifically addressed in either COPPA or the DMA guidelines.

Overall, while certain information about data privacy does seem to be available on some of the sites visited by children, it is unlikely that children will ever find it. On Foxall and Kilcoyne's (1993) model, the sites would fall either into the category of: 'consumers have privacy rights but are not aware of them. Because they assume they must provide personal data, they do not exercise control over its release'. Or 'consumers are not aware that they have privacy rights — and even if they were aware, they may or may not have a say about the collection and use of personal data' (p. 107).

Parental involvement is not always encouraged

Parental involvement

The role of the parent in the protection of children's data is heavily emphasised in both COPPA and the DMA Code. In fact, both state categorically that information on children should not be collected without specific parental permission. On every single one of the 20 websites investigated, it was, however, easily possible for a child to disclose personal information with no parental consent at all. In fact, 70 per cent of the sites made absolutely no attempt to encourage parental involvement. Piczo, cheatplanet and Popcap absolved themselves of the need to involve parents by stating on the data collection page that the site was only intended for those over 13 (piczo and cheatplanet) or 18 (Popcap). (As these sites are among the most visited sites by the children under 13 in our survey, such a warning clearly has little effect.) Three sites which were most obviously targeted at a child-only audience (Disney, Habbo Hotel and MyScene) made more effort than others. They specifically asked children to provide a parent's e-mail address if they entered their age as under 13 (Disney and MyScene) or 16 (Habbo Hotel) (Figure 6).

When the researcher entered a 'parental' e-mail address on each of these sites, a message was sent very promptly explaining that the child had registered and to encourage the parent to read the privacy policy and offering the parent the option to cancel the child's registration. However, and it is a very big however, it was perfectly possible to register for a desired activity using a false parental e-mail or, indeed, to give a false age, thus rendering this provision for parental involvement utterly useless in practice.

This poses an interesting question for the industry. If parental involvement is to play a major role in ensuring children's data privacy — how can this be effectively achieved? The current practice of asking

The screenshot shows a web browser window with the URL 'https://www.habbo.co.uk - Habbo - Registration - Email address - Microsoft Internet Explorer'. The page has a 'HABBO' logo at the top. Below the logo, there are navigation tabs numbered 1 to 5, with tab 3 being active. The main content area is titled 'REGISTRATION' and contains a cartoon character pointing to the email fields. The form asks for 'YOUR EMAIL ADDRESS' and 'PARENT'S EMAIL ADDRESS'. There is a checkbox for 'Yes!!! I want the latest Habbo news sent straight to my inbox!'. The page also includes a 'Cancel' button and a 'CONTINUE' button. At the bottom, there is a copyright notice for 2006 Solake Corporation Ltd.

Figure 6: Collecting parent's e-mail

Enforceability of parental consent may be impossible to achieve

the child for the parent's e-mail address is clearly inadequate. In fact, the practice actually contravenes Section 19.33 of the DMA Code, which states quite clearly that personal information from parents must not be collected from children.

While parental involvement appears, in theory, a sensible way to resolve the issue of whether children should be protected or accorded the right to choose, the enforceability of parental consent in practice remains highly questionable and may simply be impossible. Livingstone and Bober,²⁹ in their comprehensive review of children's online activities, found that children are often unwilling to involve parents in their internet activities as they see *this* as an invasion of their privacy. In their survey, 69 per cent of 9–17-year-old daily and weekly users of the internet said that they minded their parents monitoring their internet use; 63 per cent of 12–19-year-old home internet users had taken some action to hide their online activities from their parents and 40 per cent had used the internet to engage in identity play. During a time of adolescent development when young people are trying to establish their own identity among peers and away from the family, the immediate privacy threat from parents can be viewed by some young people as much more significant than the distant threat of their personal details being used by someone they do not know or care about.

Conclusion

Children's rights are ambiguous

The concepts of knowledge and control have formed a useful basis for defining the data protection rights of adults. These are, however, problematic concepts when applied to children. This is partly because the very nature of the rights of the child is ambiguous. Children are viewed alternatively as having the right to be protected and the right to

be heard. Current best practice encourages the involvement of parents as mediators between website owners and children. Our review of the top 20 sites visited by UK 9–13-year-olds shows that children are currently offered neither sufficient information on privacy issues nor sufficient control over how that information is used. Most importantly, the notion of involving parents in the process of protecting children's data privacy is shown to be highly flawed.

Future research

Time for a rethink?

It is hoped that this paper may stimulate the industry and its regulators to rethink the issue of protecting children's privacy online. The next step is to involve both children and parents in this research to assess how informed they are on child data protection issues and to seek their views on future best practice guideline.

Acknowledgments

This research has contributed to a larger ongoing project with The National Consumer Council and Childnet International.

References

1. Childwise (2006) 'Monitor Trends Report', available at www.childwise.co.uk/trends.htm, accessed 10 December 2006.
2. Sutherland, A. and Thompson, B. (2003). *Kidfluence*, McGraw Hill, New York.
3. Lindstrom, M. and Seybold, P. (2003). *Brandchild*, Kogan Page, London.
4. Siegel, D. L., Coffey, T. J. and Livingston, D. (2004). *The Great Tween Buying Machine*, Paramount Market Publishing: New York.
5. Chordas, A. (2001) 'A new generation in the crosshairs'. *Best's Review*, February.
6. Martensen, A. and Groenholdt, L. (2006) 'Understanding tweens' needs and motives for mobile phones: A means-end chain approach', *Proceedings of ICORIA*, June 30th – July 1st, Bath, UK.
7. Story, L. and Pfanner, E. (2006) 'The future of web ads is in Britain', *New York Times*, 4 December.
8. Brandeis, W. (1890) 'The right to privacy', *Harvard Law Review*, Vol. 4, p. 193.
9. Westin, A. (1967a) 'Legal safeguards to insure privacy in a computer society', *Communications of ACM*, Vol. 10, No. 9, pp. 533–537.
10. Westin, A. (1967b). *Privacy and Freedom*, Athenaeum, New York.
11. Wasserstrom, R. A. (1978) 'Privacy: Some arguments and assumptions', in Bronaugh, R. (ed) *Philosophical Law: Authority, Equality, Adjudication, Privacy*, Greenwood Press, Westport, CT, pp. 148–166.
12. Wood, D. M. (ed) (2006). *A Report on the Surveillance Society*. For the Information Commissioner by the Surveillance Studies Network. (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf).
13. McNealy, S. (1999) Comment to Wired.com, 26 January (<http://www.wired.com/news/politics/0,1283,17538,00.html>).
14. Goodwin, C. (1991) 'Privacy: Recognition of a consumer right', *Journal of Public Policy and Marketing*, Vol. 10, No. 1, pp. 149–166.
15. Foxman, E. R. and Kilcoyne, P. (1993) 'Information technology, marketing practices and consumer privacy: Ethical issues', *Journal of Public Policy and Marketing*, Vol. 12, No. 1, pp. 106–119.
16. Milne, G. R. and Rohm, A. J. (2000) 'Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives', *Journal of Public Policy and Marketing*, Vol. 19, No. 2, pp. 238–249.
17. Phelps, J., Nowak, G. and Ferrell, E. (2000) 'Privacy concerns and consumer willingness to provide personal information', *Journal of Public Policy and Marketing*, Vol. 19, No. 1, pp. 27–41.

18. Dinev, T. and Hart, P. (2003) 'Privacy concerns and internet use — A model of trade-off-factors', *Proceedings of Academy of Management Conference*, Seattle, D1–D6.
19. Awad, N. F. and Krishnan, M. S. (2006) 'The personalisation privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled on-line for personalisation', *MIS Quarterly*, Vol. 30, No. 1, pp. 13–28.
20. Armitage, C. J. and Conner, M. (1999) 'The theory of planned behavior: Assessment of predictive validity and perceived control', *British Journal of Social Psychology*, Vol. 38, No. 1, pp. 35–54.
21. Azjen, I. and Driver, B. L. (1991) 'Prediction of leisure participation from behavioral, normative, and control beliefs: An application of the theory of planned behavior', *Leisure Sciences*, Vol. 13, No. 3, pp. 185–204.
22. Wortman, C. (1975) 'Some determinants of perceived control', *Journal of Personality and Social Psychology*, Vol. 31, No. 2, pp. 282–294.
23. Caudill, E. M. and Murphy, P. E. (2000) 'Consumer online privacy: Legal and ethical issues', *Journal of Public Policy and Marketing*, Vol. 19, No. 1, pp. 7–19.
24. Stewart, K. A. and Segars, A. H. (2002) 'An empirical examination of the concern for information privacy instrument', *Information Systems Research*, Vol. 13, No. 1, pp. 36–49.
25. Smith, C. (2003) 'Corporate social responsibility: Whether or how?' *California Management Review*, Vol. 45, No. 4, pp. 52–76.
26. Archard, D. (2004). *Children: Rights and Childhood*, Routledge, London.
27. Archard, D. (2006). *The Moral and Political Status of Children*, The Author Journal Compilation, London, ippr.
28. Kouzeleas, N. (2005) 'Direct marketing and children — How far can you go?' *Database Marketing and Customer Strategy Management*, Vol. 12, No. 3, pp. 257–265.
29. Livingstone, S. and Bober, M. (2005). *UK Children Go Online: Final Report of Key Project Findings*, London School of Economics and Political Science, London.

Appendix A

Structured Observation Guide

Nature of data collected

Can a child browse through the site without having to disclose personal information?
If not, what kind of information is collected?

Knowledge

Is a privacy policy posted on the website?
Does the policy explain why data are being collected?
Is this information given at point of data collection?
Is information given on home page?
Is it prominent?
Is it understandable by a child?
Is the child informed that parental consent is required for data collection?

Control

Is access to website contingent on divulging information?
Are children enticed to give information with prospect of special prize or reward?
Can a child's information be posted publicly without parental consent?
Does privacy policy state that giving information is voluntary?
Is the child alerted to the use of cookies?
What choices are children given in terms of information being passed on to third parties?

Parental involvement

Is parental consent required?
How is it obtained?
How is it verified?
Does privacy policy explain to parents how they can access information given by their child?
Does privacy policy provide information to parents on interactive activities?