

**ALL IN THE DATA FAMILY:
CHILDREN'S PRIVACY ONLINE**

Written by: John Lawford
Research: Mani Taheri
Public Interest Advocacy Centre
1204 - ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

September 2008

Copyright 2008 PIAC

Contents may not be commercially reproduced.
Any other reproduction with acknowledgment is encouraged.

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

ALL IN THE DATA FAMILY:
CHILDREN'S PRIVACY ONLINE

1-895060-86-9

Acknowledgement

Financial support from Industry Canada to conduct the research on which this report is based is gratefully acknowledged. The views expressed in this report are not necessarily those of Industry Canada or of the Government of Canada.

EXECUTIVE SUMMARY

This paper reviews the privacy risks posed to children when commercial entities begin targeting children through their personal information on the Internet. Children's websites overwhelmingly expose their private information without their informed consent or that of a parent or guardian, under the guise of joining or enjoying websites that are designed to be online playgrounds.

The paper is informed by a qualitative research study performed with young volunteers aged 11-17 in a controlled computer laboratory environment in Toronto, Canada, in which they were allowed to engage in any Internet activity. This behaviour was monitored and tracked (in accordance with full disclosure and proper research ethics). Participants were also engaged by a moderator in a discussion of online privacy in relation to their computer use.

This paper concludes that the current legislative privacy framework in Canada and the important effect of limited privacy laws in the United States (from where most websites are either based or draw their privacy standards) is inadequate to protect children's online privacy to a standard that is appropriate. As a result, this report recommends that Canadian privacy law, and chiefly the *Personal Information Protection and Electronic Documents Act* (PIPEDA) be amended to add specific rules in relation to the protection of children's privacy.

First, there should be a general prohibition on the collection, use and disclosure of all personal information from children under the age of 13. This age marks a rough threshold for children to be considered capable of making decisions about themselves (what is known in medical law, for example, as being a "mature minor"). The benefit of ubiquitous information-based web tools is outweighed by the harm to the privacy and developmental needs of children in this age group. Parents presently are not actively monitoring children's privacy choices at this age and privacy policies and terms are too difficult, vague or purposely unspecific for either parents or children to even approach the level of understanding required to consent to this model.

Second, for young teens aged 13-15, websites should be permitted to collect and use personal information, with the consent of the teen and the explicit consent of a parent for the benefit of the child and solely in relation to that website or service and should not be permitted to further disclose their personal information.

Third, for older teens aged 16 to legal majority (18 or 19), websites should be permitted to collect and use personal information, with the consent of the teen. Such websites should be permitted to disclose the personal information of the teen only with the opt-in consent of the teen and explicit consent of a parent. Any website undertaking such collection and using such personal information (and disclosing it as per explicit consent instructions, if allowed) should

demonstrably conform to all present requirements of Canadian privacy law, in addition to these new age restrictions.

Once children reach 18 years of age (depending upon the province, this is the time at which persons in Canada reach the legal “age of majority” and are legally considered adults for most purposes, including making contracts), websites that have collected and used personal information (or that have been transferred the child’s personal information with explicit consent during this period) should no longer be permitted to retain the information gathered during the child’s “legal minority” and should be required to remove the information immediately (a privacy “get out of information jail free card”) unless the newly adult person gives his or her explicit consent to the continued collection, use, and (should they agree) possible future disclosure of their personal information gathered during their minority.

These requirements address the present reality of “immersive advertising”, social networking and other websites and services that routinely perform “market surveillance” as a business model. The requirements are designed to and seek to avoid encouraging children to enter this “data family” until they are capable of appreciating, to a reasonable degree, that they are ready for the responsibility. Even when a “mature minor” in the 16-17 year old age bracket makes the decision to allow collection and use of his or her personal information, this information is safeguarded, as it is limited from being further disclosed (unless there is explicit consent of the child and parent to do so). As a child reaches the legal age of adulthood, he or she is given a final chance to consider the implications of permitting such businesses to retain the information that was compiled during their legal minority. If they do not wish their childhood “data record” to follow them, they may simply walk away from the compiled information, confident that it will not be used as a basis to re-target them with advertising or other promotional material in their adulthood.

Businesses, during a child’s minority, therefore would not be able to disclose any personal information, unless the child or a parent or guardian explicitly consented to such a disclosure and only during the years 16-age of majority. It is expected that the effect on some businesses that are heavily funded by personal information-based advertising would be a likely retreat from offering some services to the youngest of children.

These simple rules are clear and easy for businesses to follow. The rules would be easy for the Office of the Privacy Commissioner of Canada to explain and would allow the Office to conduct regular audits of the personal information handling of websites targeting children. In addition, the report suggests that the Office of the Privacy Commissioner be given fining powers to enforce the new children’s privacy rules.

The rules as proposed would still permit children to use online playgrounds (at any age) provided that the website found ways of supporting itself from non-targeted advertising or selling profile information of users. Business models relying upon “immersive advertising” would continue to be able to exist, however, they would not be permitted to target advertising to children based on the profile they have built up from the child’s use of the website.

Other more specific rules are proposed for social networking sites, given these sites’ attraction to teens and the immense amount of personal information they collect. Firstly, teen users would benefit from the strictest privacy settings available on a website by default. Second, the social networking site would be prohibited from allowing lookup services (even to members within a site) that were able to return lists of children. Third, children would be allowed to sign up for social networks with a pseudonym.

Social networking services would be available starting at age 13, as before that time, the child’s personal information could not be collected, used or disclosed, even with explicit consent, to any third party (including those who also were members of a social network). For teens aged 13-15, if a social networking site wished to post limited access profiles (access only from within their website) they would be required to seek explicit consent to this limited internal use from the teen and parent. Effectively, social networking sites could not seek to fund their services for the 16-17 age group from third party advertising, unless the advertising were general demographic (non-targeted) in nature, or explicit consent had been obtained from the teen and a parent or guardian. These older teens could, however, sign up to and use social networking without their parent’s consent.

The Report also makes several recommendations involving increasing the readability and simplicity of privacy notices for children and adults; adoption of a privacy rating system that is simple and has graphical representations of privacy threat levels; better education of children and parents in online privacy protection and rights. There should also be efforts to coordinate privacy rules across jurisdictions so that any Canadian standards are not easily avoided. Finally, governments should develop or support the creation and maintenance of non-commercial online spaces for children.

Given the prevalence of personal information collection, use and consent of children already on the Internet, only such clear, enforceable rules can make a significant impact in returning the Internet to children as a safe place to play and learn without first becoming an unwitting member of the “data family”.

TABLE OF CONTENTS

INTRODUCTION	9
Focus Group Findings.....	10
Methodology.....	10
Statement of Limitations.....	12
Kids’ Views of Privacy Online.....	12
Kids Reading Privacy Policies – Not.....	19
Business Models of Children’s Websites	21
The Standard Third-Party Targeting Business Model	21
The “Immersive Advertising” Model	23
Example: Neopets	24
Overt Market Research Surveys	27
The Social Networking Model.....	28
Example: Facebook.....	31
Risks of Overcollection of Data and Profiling to Children.....	38
Criticisms of Behavioural Marketing to Children	41
Children’s Privacy Online - The Legal Context	43
Voluntary Ad Industry Standards	43
Canadian Standards.....	43
U.S. Standards.....	46
Legal Standards – Overview.....	48
Legal Capacity, Consent and Children in Canada	48
<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i>	50
PIPEDA and Children.....	50
Consent under PIPEDA	51
Principle 4.3.3 – “Necessary for the Purpose”.....	56
Reasonableness under s. 5(3).....	57
FOREIGN LEGISLATION	59
The United States’ Children’s Online Privacy Protection Act.....	59
Criticisms of COPPA Approach.....	61
The UK’s Dual Approach Part I - The Privacy and Electronic Communications (EC Directive) Regulations	63
The UK’s Dual Approach Part II - The <i>Data Protection Act</i>	63
The Way Forward: Legal and Policy Recommendations	66
Clarifying Children’s Consent under PIPEDA.....	67
Recommendation 1: Amend PIPEDA to provide clear consent rules for children.....	69
Children Under 13.....	70
Younger Teens (13-15).....	70
Older Teens (16 to majority).....	71
Recommendation 2: Visible, clear and understandable signs of collection, use and disclosure	73
Recommendation 3: Draft privacy policies children can understand	74
Recommendation 4: Specific regulations for social networking sites	75
Recommendation 5: Privacy Commissioner should enforce the new regime with new fining power; Audit powers	75

Recommendation 6: Government should Support or Create Non-commercial Online Playspaces	76
Recommendation 9: Coordination and Promotion of Child Privacy Rules Worldwide	76
Recommendation 10: Online Privacy Education for Youth	77
Conclusions.....	77
Appendix 1 – Environics Research Group Report on Focus Groups	79
Appendix 2 – Neopets Privacy Policy	80
Appendix 3 – Facebook Privacy Policy.....	85
Safe Use of Facebook	85
Facebook's Privacy Policy	85
EU Safe Harbor Participation	86
The Information We Collect	86
Children Under Age 13.....	87
Children Between the Ages of 13 and 18	87
Use of Information Obtained by Facebook.....	87
Sharing Your Information with Third Parties.....	88
Links	90
Third Party Advertising	90
Changing or Removing Information.....	90
Security	91
Terms of Use, Notices and Revisions	91
Contacting the Web Site	91

INTRODUCTION

Over the past few years the Internet has become a primary source of communication, education and above all, play, used by Canadian youth. However, few children or parents realize the extent to which advertising, online profiling and disclosure of private information over the Internet shapes and funds this vital communications network. As a result, PIAC undertook this study to examine children's spaces on the Internet and the use of children's private information to build and fund these spaces. While similar studies had been performed on this scene in other countries, no comprehensive Canadian study had been done.

Another unique feature of the present report is the opinion of young Internet users on privacy, which PIAC, with Environics, attempted to capture, in focus groups conducted with Canadian children while they were actually using their favourite Internet sites and services, such as Facebook, MSN and YouTube.

The focus groups found that most children are aware of many online dangers, such as approach by adult strangers in chatrooms, and requests to "meet in real life", mainly due to the information given them through parents, school speakers, media stories or discussions with teachers. Those surveyed reported that they take this safety information very seriously and have taken it upon themselves to be well-prepared and protect themselves when online. These well known risks are not further discussed in this report, however, it is acknowledged that they are of paramount importance and that parents, teachers and legislators should not become complacent in relation to improper direct solicitation of children's information.

Less well understood by focus group participants, however, was the "privacy bargain" each child was entering into to participate in their favourite online playgrounds and websites and services. It is this information exchange that this report seeks to illuminate for Canadian children and their parents. References to the focus group findings are made throughout the report and the entire Environics report on the focus groups is reproduced in the electronic version of this report as Appendix 1.

A brief explanation of the business model of children's websites and services on the Internet then is given which concludes that the dominant feature of such websites is that they are advertising-supported – not simply by demographic ads but by targeted advertising (advertising geared to the individual child) and market research on children's product and other preferences.

Views from privacy advocates, sociologists and other researchers on this personal information-driven business model then are detailed. Risks from such a model to children's privacy then are briefly discussed.

The report then focuses on the legal framework for privacy protection of children in Canada and in particular the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The inquiry also looks at the effects of the children's online privacy law of the United States, known as COPPA, as this country is the home of many of the most popular children's websites and services, or for those based in Canada, appears to profoundly inform the privacy policies of Canadian websites. The weaknesses of the present legal framework in Canada are then noted in relation to children's privacy in this environment.

The report then makes concrete recommendations to improve privacy laws in Canada to protect children's privacy online in relation to personal information collection, use and disclosure for the purposes of advertising and market research.

Focus Group Findings

The Public Interest Advocacy Centre (PIAC) and Environics Research Group (Environics) conducted focus groups with children and teens in Toronto in November 2007.¹ The participants were divided into two groups, aged 11-13 and 14-17, based on guidance from the facilitator, who suggested that younger children would defer to the opinions of old teenagers if the groups had a broader age range. Although the number of participants in the focus groups was small, totalling only 10 participants in total, care was taken to ensure as broad as possible a range of geographic and socio-economic backgrounds were represented. Fuller information on the methodology of the focus group research is contained in the Environics Report on the focus groups, found below and in the full Environics Report at Appendix 1.

Methodology

The qualitative component of the focus group research consisted of two focus groups conducted in Toronto, one with youth aged 11 to 13 years and one with youth aged 14 to 17 years. Both sessions were conducted on Saturday, November 24, at 12:00 pm and 2:30 pm, respectively. Each session lasted approximately two hours.

Participation in Groups			
Date	Age group	Recruited	Participated
November 24,	11 – 13 years	8	4 (2 boys, 2 girls)

¹ The full report is S. Preiner [also the focus group facilitator], "All in the Data Family? Databases, Children and Profiling: A Qualitative Exploration" Environics Research Group (January 2008). The full report is reproduced in the electronic version of this report at Appendix 1.

12:00pm			
November 24, 2:30pm	14 – 17 years	8	6 (3 boys, 3 girls)

A qualitative group method called the Intensive/Interaction Workshop Group Method was employed in these discussion groups. This method is similar in many ways to the traditional focus group and is a qualitative group approach. The key difference between the two approaches is that, with the use of the workshop approach, participants who may not be skilled at sharing their thoughts, beliefs and values in a public setting are helped by the research process to do so in a comfortable way. This approach improves the depth of the research findings and allows each participant to share to the best of their ability.

In the workshop approach, participants are periodically given paired or individual tasks on which they work for a short time. After the pairs have completed their task, they then return to the discussion table to share their ideas, including the similarities and differences of their thought processes. This approach allows participants to quickly come to grips with various aspects of their own ideas and issues related to the research topics, which in turn makes it easier for them to discuss and present views and conclusions within the sessions. (Please see Appendix for further detail.)

Eight participants were recruited for each group with an expectation that a maximum of six would participate. This allowed for some re-screening before the young people are invited into the room so that those who are most articulate and socially comfortable were invited to participate while those who are uncomfortable or who change their mind about participation could be identified before the group begins. All participants received parental permission in writing to enter the group. The recruiters spoke with both the parents of young people and the young people themselves before confirming their participation to be sure that all parties understood the discussion format and that this is a research project – nothing is being “sold” or “advertised” in these sessions. All participants and their parents were informed that the sessions would be audio and video recorded and that this material would be used in the analysis of this work. All parents signed a release for this recording to take place.

Both groups were conducted in purpose-built focus group facilities, and were videotaped and recorded. In each group a computer with web access was available for each of the participants. The computers were set to record sites visited by each participant and there was a monitor in the observation room to allow observers to watch the activity of each participant one at a time. An IT technician was on-site during both group sessions to ensure that qualified technical support was immediately available should problems arise.

An incentive of \$60.00 was provided to all those recruited on the date of the focus groups. All incentive monies were given to the participants in the group not to their parents.

Both groups were moderated by Sally Preiner, Senior Consultant, Qualitative Innovation, Environics Research Group. All qualitative research work was conducted in accordance with the professional standards established by the Marketing Research and Intelligence Association (MRIA) (previously the Professional Market Research Society and the Canadian Association of Market Research Organizations), as well as applicable federal privacy legislation (PIPEDA).

Statement of Limitations

The objectives of this research initiative are exploratory and therefore best addressed qualitatively. Qualitative research provides insight into the range of opinions held within a population,² rather than the weights of the opinions held, as would be measured in a quantitative study. The results of this type of research should be viewed as indicative rather than projectable. The intent of this research is to provide insights into the range of issues and opinions, and not the weight of those issues.

PIAC buttressed the qualitative research with extensive secondary research and primary research in the form of interviews with stakeholders.

Kids' Views of Privacy Online

Despite the overt monitoring of conversations and Internet use, the participants displayed a high level of comfort with the monitoring and appeared to soon use the Internet in an “everyday way” within minutes. More information about the methodology is contained in the Environics Report, however, it is worth noting here that the Internet connections, while monitored, were in no way filtered, nor were the participants told which sites or services to use, except for a ban on e-mail.

² The 11-13 year old group represents a diversity of youths, some living in affluent neighbourhoods in downtown Toronto and attending private school some in public schools from less affluent neighbourhoods in the downtown and a similar mix of children from affluent and less affluent suburban centres who attend public schools. Occupations of parents included a range from retail sales, accounting clerk and self-employed with a number of homemakers (presumably with a working spouse). The majority of these children had a computer in their own room and the rest had access to a shared family computer.

The 14-17 year old group was similarly diverse but slightly different: most children came from suburban areas (affluent and less-affluent) and although different neighbourhoods, all appeared to attend public schools. Occupations of parents ranged from data entry clerk to social worker, to secretary and small business owner. In this group, most children had access to a shared family computer rather than one in their own room.

Based on the conversations in the focus groups, it appears that participants perceived the notion of staying safe online to represent:

- Limiting access to certain personal information, including full name, address, school location and physical descriptions;
- Watching out for people who seem potentially dangerous;
- Not meeting people in real life that they have met online;
- Avoiding involvement with cyber-bullying, and;
- Avoiding viruses.³

However, even though most of those surveyed found it necessary to limit providing their private information online to other individuals, those same participants did not perceive there to be many potential risks associated with providing personal information in public online spaces or to website administrators and corporations they consider to be safe,⁴ such as Facebook, Webkinz and YouTube.

From the qualitative research in this study and on reviewing other studies, it appears that children and teens see the online world as an extension of the offline world, rather than as a separate space with different rules.⁵ Thus they may be more likely to transpose their trust evaluation mechanisms to the online world than an adult. Most children are taught from an early age to be cautious around strangers and not to reveal identifying information, to limit what they do and say in public spaces while being encouraged to be open with loved ones and more free with their behaviour in the home or school. As a result, children appear to trust interactions with people they know “in real life” and to avoid giving out information that, in real life, might be dangerous or lead to privacy invasions.

This may help to explain why we found that children tend to trust certain larger, better known websites more than others, especially those that are frequented by a large core of users (generally their peers), which are run by major corporations,

³ Environics Report, Appendix 1, slide. 28.

⁴ Environics Report, “Detailed Findings”, p. 18.

⁵ See Valerie Steeves [research advisor on this report]: “The Watched Child: Surveillance in Three Online Playgrounds”, Proceedings of the International Conference on the Rights of the Child (Montreal: Wilson Lafleur, 2007). “El niño observado: vigilancia en tres sitios de juegos de niños en Internet”, Actas de la Conferencia Internacional sobre los Derechos del Niño (Buenos Aires: Universidad de Buenos Aires, 2008): “Although children see it as a useful tool for learning, the Internet is primarily a social space to them, and the boundaries between it and the real world are fluid.” (citing SONIA LIVINGSTONE, “Children’s Privacy Online: Experimenting with Boundaries Within and Beyond the Family”, in KRAUT, R. E., M. BRYNIN and S. KIESLER (eds.), Computers, Phones, and the Internet: Domesticating Information Technology, New York, Oxford University Press, 2006; VALERIE STEEVES, Young Canadians in a Wired World, Phase II: Trends and Recommendations, Ottawa, Media Awareness Network, 2005.; LESLIE REGAN SHADE, NIKKI PORTER AND WENDY SANCHEZ, ““You Can See Anything on the Internet, You Can Do Anything on the Internet!”: Young Canadians Talk About the Internet”, (2006) 30(4) Canadian Journal of Communication, 503-526; SONIA LIVINGSTONE & MAGDALENA BOBER, UK Children Go Online: Listening to Young People’s Experiences, London, Economic and Social Research Council, 2003.

or those that pose no “real” threats to their informational privacy, as they perceive it. It appears children trust these sites as they do home or a friend’s house or school environments, where they have been “allowed” to go and where peers and parents encourage them to try more overt behaviour.

This may also help to explain two seemingly contradictory attitudes of the focus group participants. First, there was a surprising level of awareness of tracking of their clickstream data, even on these trusted websites, both by the target website and any third-party advertising “partners”. That is, the participants knew that the “main” or initial website not only would have some details about them (surmising that these clicks would be linked to information they had provided voluntarily in order to access the website (such as their e-mail address in a registration process)) but also had an inkling that other third party sites could track their movement on the Internet. They also understood this was being done to advertise and ultimately to make the websites involved money. Understandably, the details of the actual mechanics of this process on the Internet were poorly understood and were expressed in some generalities and linked to the one concrete information management decision they had made – namely to provide personal information during a registration process.

Second, it appeared that the participants were alternately unconcerned with this tracking and were resigned to it. Effectively, they thought that the information would really lead to no real harm. They appeared not to be concerned with surveillance of their activities *per se*, unless it led to eventual identity theft or harassment. Still, they had some concerns with surveillance when it was made obvious and personal to them.

First, regarding tracking, focus group participants said this:

“The second you get an e-mail then they know your e-mail address. And they can determine, say, you go to work, you put that in and if you go to work then you put your e-mail address cause you use it a lot for your job. Then they’ll figure out where you work because when it’s your home, they can trace that, so then they know where you live and where you work. Then where you live, they can get your names. And then they know family name, every individual name, middle name and all that stuff. And then from there, they can get to everything from like your date of birth from what brands you bought last year.” (11-13 years)

“They monitor where you go so that, when you type a keyword it’s kind of scary and like spooky at the same time when you get like advertising results. They’re trying to advertise, get as close to what you’re trying to do so they’re trying to advertise to you and sell you something based on what you type in.” (14-17 years)

“If you go to a site pretty frequently they might have in their on-line files something that has your computer, maybe a number or something in your computer that shows what you search and stuff like that on their sites. So they can market their site to meet the majority of what people want...to meet people’s needs or something like that.” (14-17 years)

“They make money off you. It’s not paying you anything. It’s a place where you can share your information but they majorly incorporate it into their own business and they make money out of it.” (14-17 years)

Second, regarding acceptance/resignation (or harm) to the data surveillance:

I guess I don’t really get impacted by any negative effects of giving out my information. (14-17 years)

“It matters but to me it’s not that big of a concern because really no matter what kind of information you give out, if someone really wants to find out about you, they can.” (14-17 years)

“Probably, maybe safety would be more of a concern as I’m older maybe if you had, like, a family or something and you were looking out for people.” (14-17 years)

“Not to say that it doesn’t concern me as much as it will when I have a credit card and there’s a lot of things to worry about like identity theft.” (14-17 years)

These attitudes in fact can be reconciled if the children view the online world as a structured environment that is “just that way” and that they are not in a position to change it. In fact, it appears that these focus group participants were willing to provide personal information, which they have been told not to provide to individuals, to these corporations because they have been encouraged by friends’ and family approbation of the sites as mainstream, and that this disclosure would not lead to risks. The surveillance aspect, while “scary” or “spooky” when it provided a concrete advertising result on a webpage, was not objectionable in itself. Internet surveillance at some level appears normalized.⁶

⁶ At the close of the 11-13 year old focus group, one participant took the opportunity, however, to describe what is probably a reference to the failed Total Information Awareness program in the U.S., showing a chilling suspicion that state agencies might be interested in private information of even children:

R. *For a while, I thought phone lines were secure except when people tap them. And then government agencies can tap them then I realize that also everything that sucked up in the (inaudible). I forgot what it stands for but it’s a CIA operated satellite, it just sucks up everything and, you can’t store all the stuff so it picks up key words and programs (inaudible) after 911 and all that stuff. Now we talk about that stuff, say you’re talking about a video game, where you need to play something to bring down a wall to get to a new area. Only the key words from that can be brought up and (inaudible, voice too low.). (11-13)*

While children in the focus groups may be becoming resigned to a certain level of abstract (from their viewpoint) surveillance, this is not to say that they were comfortable with more direct evidence that they were being surveilled. When it was made clear to them in the research recruitment process and again at the research facility that their online actions would be tracked by software, and watched on monitors behind one-way glass where observers could monitor their every keystroke, they did feel uncomfortable at the loss of privacy. None of the children, however, stated that they changed their online activity:

M: Okay, and come on back. Just leave the computers on and come on back. Thanks. Thanks everybody. Did anybody learn anything about themselves or about the internet as you were doing this today because sometimes you can do it in a different environment and you suddenly notice something about yourself? How about you?

R: Did I notice anything about myself?

M: Yeah, or were you aware of something different that you were doing?

R: I don't know. I went to Google again for YouTube I don't know because I forgot the spelling of it.

M: Okay, how about for you?

R: *Sort of because I knew I was being watched so I still did the same things I usually do. I just felt kind of awkward with people watching me.*

M: Yeah, so being watched can be kind of uncomfortable, that's for sure. How about you, B?

R: No, not really.

M: R?

R: I didn't do anything differently.

M: So it was the same, felt the same as usual?

R: *It didn't feel the same as usual.*

M: How did it feel differently?

M: You just don't believe that privacy exists do you?

R: *If you don't do anything suspicious, no one is really going to care. (11-13)*

R: *(Inaudible, low-talking) because someone's watching what you're doing, analysing it (inaudible, low-talking).*

Part of the focus group participants' ability to rationalize what they know to be a certain level of surveillance may also stem from a belief that corporations only track their behaviour in the aggregate. In other words, they have a not-unreasonable belief that they are just an individual tree, while the websites and advertisers are interested in the forest:

M: Okay, B. what do you think? When you put information in what do they know about you, the corporations that you use when you go their sites, those are companies.

R: Me personally, all they know is e-mail address and my name.

M: Okay, R., just guessing with that information that B. gets in, what could a corporation do? How much do they really know about him? *Do they really just know his first name and his e-mail address?*

R: *Pretty much unless they really wanted to research it but why would a corporation out of all the people in the world, pick him or anybody and just what would they do with the information?*

M: Okay so if I'm getting this right, a big corporation, one that again you know, a name brand, *there would be no purpose for them in knowing more about an individual?*

R: Well they might, a group of individuals or a like, *yeah a group but they wouldn't really care about one particular person (inaudible, low-talking).*

M: D. I got the feeling you weren't so sure that they wouldn't care about an individual?

R: Well I don't really think they do care, well they care about what we think because if we don't tell them then how are they going to make money? They want to know what they can do to improve the site so in some way they care but in other ways they don't really care about what you do. (14-17 year olds)

More research is indicated as it appears firstly that children, even while somewhat resigned to surveillance on the Internet, become uncomfortable with it when it is shown to them that surveillance is individually occurring. Secondly, it appears to take a lot to stop children from "doing what they usually do" even when they are aware of surveillance. This may either be due to a mistaken belief

that aggregate (supposedly anonymous) information is all that is collected or that children's experience of privacy may not be exactly similar to adults' – which may have implications regarding the extent to which disclosure of surveillance and other privacy-invasive practices may make any difference to children's online behaviour.

Kids Reading Privacy Policies – Not

Most participants also noted that they also did not bother to read privacy policies or Terms of Service contracts (where disclosure of personal information use is detailed) and instead just “accept” so they can enjoy the site.⁷

M: Well one thing I was interested in that we didn't talk about before, talking about safety, any of you ever go onto a site where you have to register and you have to put your first name and last name and e-mail address or something and *they usually have that really long contract thing. Have you ever read that D.? You ever read it?*

R: *Some of it.*

R: *It's too long to read.*

R: *I just browse it.*

R: *they should summarize it.*

M: B. have you ever read one of those contracty things or do you just go, I accept?

R: It depends for what site like I have an Xbox 360 and to go on Xbox Live which is playing online, there is all these agreements and stuff. I just read it to make sure that because you have to give out credit card numbers so I thought it was important but *otherwise no I just click without reading it.*

M: Was it easy enough to understand?

R: It was easy enough to understand but it took like 20 minutes to read it.

M: Were you bored with it?

R: Yeah.

⁷ Environics transcript, 14-17 year olds, p. 45:

Well you can't really argue with you because you're the one that gave it up. When you sign up for something and you don't, even if you do or don't read the contract, you signed up for it so it's like you're saying, I don't care you can have the information you want. (age 14-17)

M: Did you really read all of it?

R: Yeah because it was the first time I had given out credit card information online for an online service.

M: *R. have you ever read on of those contracts? No.* [Participant shook head]. (14-17 year olds)

These answers are entirely consonant with research indicating an extremely low number of children read privacy policies and have little comprehension of what they do read.⁸

Although many focus group participants noted that they do not feel comfortable taking any managed risks with their personal information with strangers, almost all have joined sites such as e-mail hosts or social networking sites where a minimum of information is stated to be required, such as accurate emails, names, location and date of birth and often much more.

During the course of our study we found that most of the websites targeting children of all age groups have a reputation for data collection. All of the most popular sites visited by our focus group participants required registration of some kind to have a more fully functional use of the website.

For example, the participants in our study gave the following examples of some of the disclosure they have made in order to access or use specific websites to their full advantage:

- My30seconds.com – e-mail, full name, city, country and postal code.
- Sprousefanclub.com – e-mail, parents credit card number, full name, username and password.
- Facebook – name, date of birth, hometown, hobbies, favourite music, favourite films, favourite books.⁹

Based on this, it merits more investigation of why kids routinely give out individual personal information but do not expect it to be turned into an individual profile, and whether a privacy policy is the best means of alerting them to this fact, if the site or its advertisers do so.

⁸ JACQUELYN BURKELL, VALERIE STEEVES & ANCA MICHETI, Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand, Ottawa, Privacy Commissioner of Canada, 2007. (Broken Doors). Online: http://www.idtrail.org/files/broken_doors_final_report.pdf

⁹ survey

Business Models of Children’s Websites

The question remains, then, whether the information that children reveal in their registration process, or through cookies and web beacons that allow them to be profiled poses any risk to them. This involves first an examination of how this information is used and aggregated by children’s website and third party data processors. It then requires an examination of the social desirability or “reasonableness” of allowing children’s personal information to be used in creating immersive advertising environments online (this is dealt with in the section on criticisms of the present system, below).

Regarding the business model supported by information collection, however, it is worth noting that children’s websites are overwhelmingly commercial websites. Nearly all of the websites mentioned as favourites by the focus group participants were commercial and collected personal information directly from children through a registration process.¹⁰ ; As commercial entities, they are subject to Canada’s *Personal Information Protection and Electronic Documents Act* (PIPEDA) or a “substantially similar” provincial law (in British Columbia, Alberta and Québec). The legal context of this information collection is discussed below.

The Standard Third-Party Targeting Business Model

Before describing the personal information business model now being used for many children’s websites, it is worth noting the standard target marketing model that applies to almost all commercial websites, via third party advertisers that set cookies on a user’s computer. In this model, a third party advertiser (for example, Doubleclick) places a cookie on the users’ hard drive when that user visits website with which the third party advertiser does business. This is done as part of the serving of the “banner ads” that appear at the margins of websites, and sometimes are identified as “advertisement.”¹¹

¹⁰ Examples of the “top ten” lists from focus group participants were (for ages 11-13): MSN; Google; Facebook; YouTube; Hotmail; Yahoo; Mofunzone; Family (Channel); Webkinz; Miniclip; Addictinggames; Disney channel; Ebay; Runescape; Ask.com and for ages 14-17 the top five were: Google; YouTube; Facebook; Hotmail; MySpace . All of these sites, including Google, Ask.com and YouTube, have extra aspects that can be accessed only upon registration. Others require registration to use most of the site or its major functions. See also in the context of U.K. children, A. Fielder, W. Gardner, A. Nairn and J. Pitt, “Fair Game? Assessing Commercial Activity on Children’s Favourite Websites and Online Environments” (London (U.K.): National Consumer Council, December 2007). (“Fair Game?”) at p. 23, online: http://www.ncc.org.uk/nccpdf/poldocs/NCC182r_fair_game.pdf , which found that “Close to two-thirds (26 out of 40) of the sites surveyed requested personal data, either as an option of as compulsory in order to continue on certain areas of a site.”

¹¹ See the description “ONLINE PROFILING: A REPORT TO CONGRESS” prepared by the FTC at: <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> , at- p. 6

The main sites the user is navigating to with his or her browser are typically search engines and major corporate websites, and the user may be unaware that the cookies are being placed as part of the service of ads to the ad banners on the main web page. These cookies then feed information on the clickstream of a user at that site or any website that hosts the third party advertiser's cookie (that is, Doubleclick recognizes the cookie and its programming as one of its "own" anywhere on the web) and those that the user visits, back to the third party advertiser, for analysis. While cookies do not always contain personal information such as full name, they may contain some personal information such as e-mail address, if the home site asked for the address and the user provided it.¹²

The important aspect of this model is that it produces aggregate metrics, such as number of "impressions", "clicks", "conversions" (when a user actually clicks a banner ad), and "performance" (that is, when the user follows the banner link and buys a product or service advertised. These metrics are important for advertisers. The third party cookie provider also has more individual "cookie-based" reports on the individual that track the individual's surfing behaviour. This information may or may not be sold to the advertisers but remains the proprietary property of the ad serving company (Doubleclick, etc.) and allows the ad serving company to build predictive models of behaviour for the individual and guarantee at least a very fine "segmentation" of the individuals it has cookie-based reports on and at best, close to "fingerprinting" the individual (that is, being able to single this user out of all other users of a website based on the cookie trail being practically unique.¹³

This type of marketing poses a threat to online privacy as an individual does not need to click on any ads for the cookies and web bugs to collect personal data. Although these tracking agents often cannot specifically identify an individual, the information they gather for the networking advertisers does not always remain anonymous either. If the individual self identifies in any manner on a website with banner ads there is always the possibility that the website can turn and sell the information to the network advertisers. As well, depending on whether the personally identifiable information is collected and processed properly, the information may be incorporated into a URL string that is automatically transmitted to the network advertiser through its cookie.¹⁴ Children are not immune from this sort of profiling and tracking, however, some children may not have personal e-mail addresses and may share a common computer with their parents, leading to difficulties for tracking usage of children more specifically.

¹² We are indebted to Mr. Scott Nelson, COO, TruEffect, for explaining this model, and particularly the metrics, in detail after delivering PowerPoint presentations on the subject to the FTC and the Office of the Privacy Commissioner of Canada. Conversation with Scott Nelson, 7 August 2008. ("Nelson Interview").

¹³ Nelson Interview.

¹⁴ <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> - p. 8

The weakness of this model, for advertisers, is that it leaves much power in the hands of, and requires payments to the third party ad servers, such as Doubleclick. In addition, the information gathered may not be completely unique and thus may not completely identify users. Finally, the prevalence of anti-spyware and other operating privacy tools that remove cookies and related devices and code has rendered these methods less effective.¹⁵

In addition, as detailed below, due to U.S. privacy legislation (COPPA),¹⁶ third parties are not generally permitted to gather information about children under 13 without express parental permission, making it difficult for children's websites serving the youngest age groups to finance under this model.

Lastly, as detailed below, children under 18 are not competent at law to make contracts or agree to any "terms and conditions" of a website, even if offered "free" and can at any time avoid such contracts at law.¹⁷

The "Immersive Advertising" Model

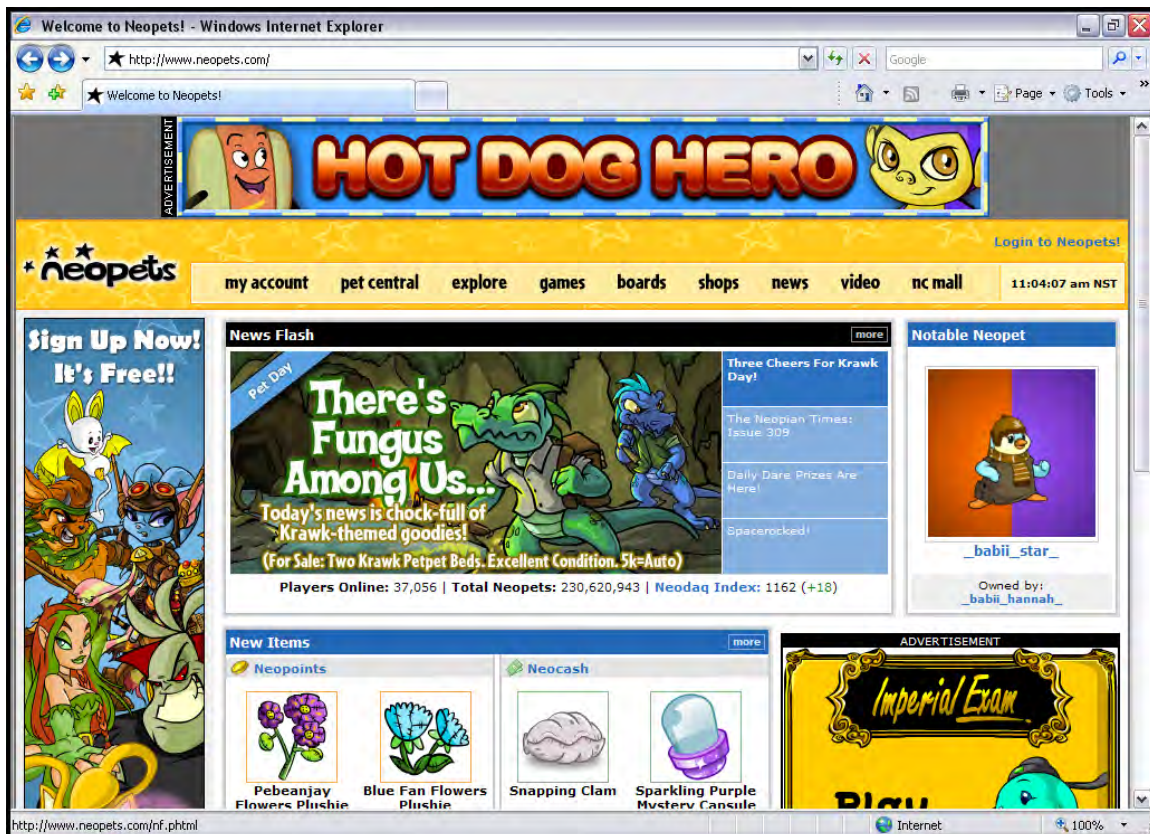
Given these constraints, the business model chosen by children's websites has not backed away from collection of children's personal information but has, perversely, greatly increased it. Under the "new" model as constrained by COPPA, companies make the websites into a virtual playground in appearance and a market research firm in function. The website then tailors the website's appearance to the profile they build of the child based on the registration information supplied (age, gender, location) and link it to progress through the site. Advertisers then pay for brand exposure in the virtual playground by either sponsoring certain games or having brands or products worked into the content of the site in an overt, or covert, way. This model is deemed "immersive advertising" and although it has spread to nearly all children's websites, was effectively led by Neopets.

¹⁵ Nelson Interview.

¹⁶ COPPA is discussed below in the section on the legal framework for children's privacy.

¹⁷ See below discussion of "Legal Capacity, Consent and Children in Canada". A note to U.K. publishers sums the conundrum up well, if providing a somewhat cynical assessment of the reality of proceeding anyways: "Under the Minors Contracts Act 1987, [which codified U.K. contract law regarding minors] most contracts do not bind a minor, although the transaction can be ratified by the minor once they reach the age of majority. The general principle, however, is that a transaction cannot be undone once it is complete (i.e. once payment has been made and the goods delivered). This leaves a potential gap between the contract being entered into and the time when the goods are paid for and delivered. During that "gap", the minor could theoretically attempt to avoid the contract. A supplier will, however, usually have the comfort of having received payment for the goods or services in advance of delivery, and therefore the onus will be on the child or his/her parents to try to seek a refund rather than simply not pay." – The Publishers Association, "CLIENT GUIDE: MARKETING CHILDREN'S BOOKS ONLINE". Online: <http://www.publishers.org.uk/download.cfm?docid=05C03C52-5D86-4B25-BEC149C309F66CAC>

Example: Neopets



(Fig. 1) Neopets.com, and other websites like it, participate in the collection of children's private data by encouraging users to identify themselves in order to further their online experience. Neopets takes the model further, however, by embedding advertising in its "immersive" environment and keeping track of individual children's progress on the site.

Neopets, now owned by Nickelodeon, itself a subsidiary of Viacom, Inc., is a typical example of a website that collects personal information in order to have a "full experience" of the site.¹⁸ (see fig. 1) Although there is some limited access to some online games without actively providing personal information to the site, the site encourages children to create a virtual pet on the site and then tend it, through feeding and other activities. Children then are invited to participate in games and other activities on the site to earn "neopoints" with which they buy food, clothing and other items for their pet. However, to adopt a pet, children must register.

Neopets was the first to subsist on "immersive advertising",¹⁹ where "ads are integrated into content rather than placed alongside it [as in a banner ad] – by

¹⁸ According to Viacom Inc.'s latest Securities and Exchange Commission Annual Filing (Form 10K), "Neopets has approximately 44 million members, and in the fourth quarter of 2007, Neopets averaged approximately 3.5 million monthly unique visitors globally." ("Viacom 10K").

¹⁹ See M. Baybak & Co. Inc., "NeoPets.com Launches Dramatic New Form of Internet Advertising" Business Wire, December 5th, 2000, online: <http://www.commercialalert.org/news/Archive/2000/12/neopetscom-launches-dramatic-new-form-of-internet-advertising-results-far> (accessed 7 August 2008) and Christine Boese, "Neopets invade the Internet

third party brands including McDonald's."²⁰ The games that are offered for play on Neopets often are branded and include cartoon product placement. (Fig. 2) Items that the pets can buy or wear are often products in the real world or from a sponsor. Other placements are downright subliminal, including one spotted during a game in PIAC's research that showed a running tickertape scoreboard with names including G. Maille (Gmail).

Neopets notes in press releases and information for marketers that this branding and product placement facility is its greatest competitive asset. In addition, the site notes the real key to this immersive advertising environment: the advertising can reach, in a very targeted way, the children who are twelve years old and under, which cannot be done through the traditional third party ad server model due to COPPA.

Neopets at first had no third party banner advertising. Some controversy erupted amongst players when banner ads were added. However, banner ads remain on Neopets and the dual method of advertising remains on this site and many others such as Webkinz, but not on some others such as Club Penguin (now owned by Disney).

Immersive games with links to corporate sponsors, as well as the banner ads on Neopets, however also provide the opportunity for disclosing personal information to third party advertisers. What is sent to each advertiser is not clear from a reading of the Neopets privacy policy. What is clear is that Neopets has discretion about what to send in terms of the child's use of the website.

World," CNN Headline News, January 7, 2003, online:

<http://www.cnn.com/2003/SHOWBIZ/01/06/hln.hot.buzz.neopets/index.html>

²⁰ Meg Carter, "Are ads on children's social networking sites harmless child's play or virtual insanity?" (The Independent, 2 June 2008). Online: <http://www.independent.co.uk/news/media/are-ads-on-childrens-social-networking-sites-harmless-childs-play-or-virtual-insanity-837993.html> (Accessed August 8, 2008).



Fig. 2. A Target-branded back-to-school game on Neopets. Note the iPod product placement.

Registration requires a **first** name, an e-mail address (to which an “activation code” is sent – before activation the site will not allow customization of the pet) and date of birth. Children are admonished to enter a correct date of birth to assist in future password retrieval if forgotten. For children in the U.S., the site also asks for city, state and zip code, although the privacy policy states that this information is not required to activate the child’s pet. This information is not taken during registration for those children identifying themselves as Canadian.

Neopets’ privacy policy is included at Appendix 2. It makes a distinction between “personally identifiable information”, “non-personally identifiable information”, “computer information” and “personal information”. This may lead to confusion for Canadian youths or adults reading the policy, as “personally identifiable information” is a concept from U.S. information and privacy law (discussed further below). However, what is more key to the privacy policy is the inclusion of a section that does allow Neopets to transfer all information the user has provided to Neopets during registration or during use of the site, including e-mail address and all other “computer information”, “non-personally identifiable information”. All a user has to do to “agree” under the privacy policy to this disclosure is to follow a link to any advertisement. This permission is included in a sentence measuring 45 words and reads as such:

Neopets never gives a user's e-mail address or other registration information to such third parties without permission, however, if you choose to "opt-in" (click on a box to receive a third party's information), to register with one of our sponsors, or not to "opt-out" (uncheck a checked box that will provide a sponsor with your information), that means you have allowed Neopets to give your registration information and other collecting [sic] information, including e-mail address, to that third party.

It is not clear if collecting information is "collected information" or some other typo. An e-mail address – often included in third party advertising cookies, can however, be shared, along with a profile of the child's activities on the site. It is also clear that to avoid collection, use or disclosure of personal information by the third party advertiser and ad server, the child must seek out their privacy policies on a separate website, read and opt-out of privacy settings – which may or more likely will not take immediate effect. This is an unlikely series of actions for a child playing an immersive game.

Overt Market Research Surveys

Professor Valerie Steeves had described another aspect to Neopets' business model that had, until recently, directly solicited children to fill out numerous third party marketing surveys that asked overly detailed questions about their preferences and lifestyles.²¹ These surveys asked children for their name, age, gender, email address, educational level, country, zip code, and ethnic background. Some surveys on Neopets have even been noted for asking children to pick items that interest or arouse curiosity in them from lists that include, gambling, alcohol and cigars.²²

However, since at least mid-August, 2008, this "Survey Shack" part of the Neopets site has been quietly removed from the Neopets website (fig. 3).

²¹ "Not Child's Play" at p. 175.

²² "Not Child's Play" at p. 176.

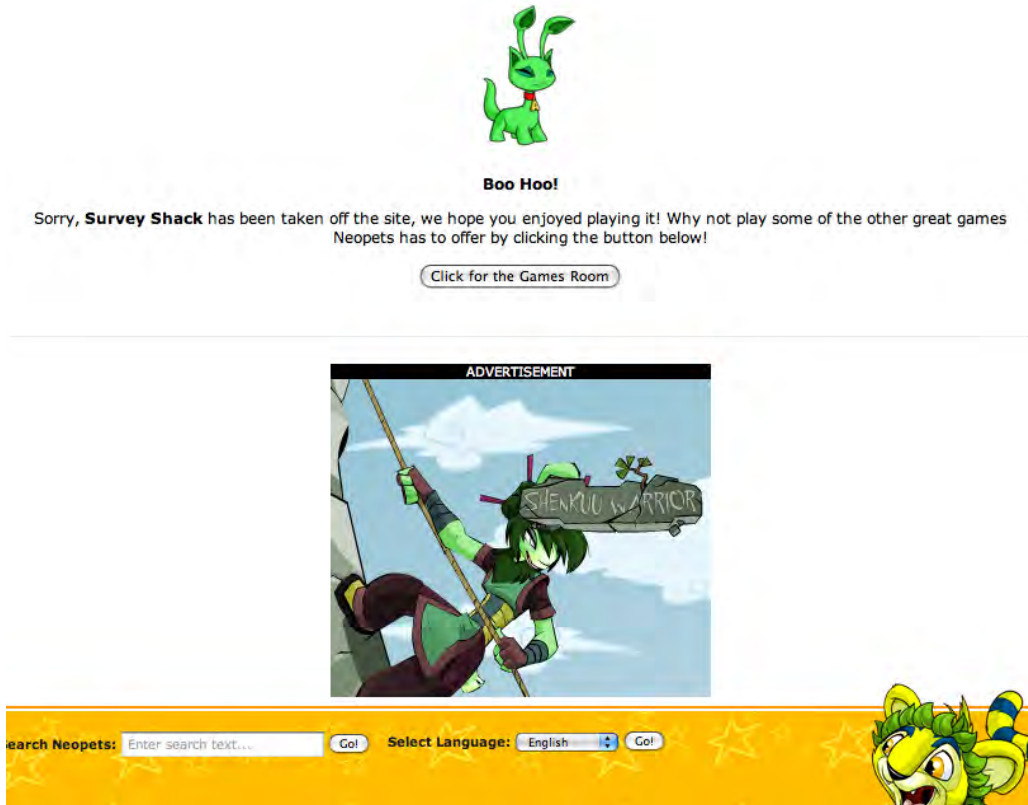


Fig 3. “Survey Shack” was quietly removed from the Neopets website some time in the summer of 2008. This page was accessed on August 12, 2008.

Survey shack may well have been removed in deference to Steeves’ criticisms or perhaps in light of Congressional investigations (House Energy and Commerce Committee) into data collection and target marketing occurring during August 2008,²³ or might be due to wholly unrelated matters. To date, Neopets has not explained the removal of Survey Shack on its Neopets game site or corporate site.

Even without overt market survey research being performed, other activities on Neopets are such research tools, dressed up in games’ clothing.

The Social Networking Model

Social networking is a global phenomenon, with millions of users across all age groups, largely concentrated in 15-20 major services. However, the demographics of social networking show a heavy weighting towards the youngest “official” users (generally those 14 and older). For example, a recent study of 49 million U.S. users shows 5,158,453 14-17 year old females used

²³ See News Release, “Energy and Commerce Committee Questions Data Practices of Network Operators” (August 1, 2008)

Myspace (3,365,442 males in this age group) versus 7,091,214 women in the 18-24 age bracket (5,226,788 of 18-24 men).²⁴ This trend is generally consistent amongst all social networking sites. Age groups older than these age groups have fewer users, dwindling with age. As a result, social networking appeals, above all, to teens and especially teen girls. This was consistent with our observations of focus groups participants – girls, and fewer boys, especially those in the 14-17 age group, accessed social networking sites immediately upon being allowed on the Internet.

The explosive growth amongst social networking sites has allowed advertisers another business model into the youth market. In Canada, Facebook has gained ascendancy over its nearest rival, MySpace, especially amongst teens. Again, this was consistent with the statements made in our focus groups.

M: You've mentioned both MySpace and Facebook, is there, are they the same or are they different? I was getting a feeling from you that they felt pretty much the same to you? How about for you? Are they the same or are they different?

R: They're like mostly the same. I've seen people use MySpace but I don't so from what I know, it's basically the same concept but maybe like because Facebook is probably now more popular than MySpace maybe then they have more applications and stuff that will interest more.

M: Any idea why it is more popular? What makes it more, looking for the difference?

R: Because it's newer. Teenagers they just like being up with what's new.

M: R., any idea, any thoughts of the difference between MySpace and Facebook?

R: I don't know I guess some people probably don't like MySpace because of the, I don't know what word to use, the general atmosphere of it. It's usually like grade eight school kids showing off.

M: Can you tell me about the atmosphere?

R: Well I guess it's different. You can't really use one to show on the website but some of it's just like, I don't want to use the word evil but like I

²⁴ Rampleaf survey reported at Richard MacManus, "Study: Women Outnumber Men on Most Social Networks", (July 29, 2008), online: http://www.readwriteweb.com/archives/social_networks_women_outnumber_men.php. Full spreadsheet results available at: http://business.rampleaf.com/xls/socialnetwork_friend_data_080729.xls

think it's sort of juvenile. Probably Facebook is probably more mature because it's not just a bunch of flashy graphics everywhere.

M: Okay, thank you.

R: It also has new tools like every time, like you know ...

M: Which one?

R: Like Facebook because they add in stuff like new tools to sort of contact each other.

R: More organized.

M: And the organization of it?

R: Yeah.

R: Yeah I guess it's just not as sloppy.

M: Not as sloppy?

R: And even in Facebook you can change the stuff like you can change the layout of the page if you want to.

M: Sorry, Danielle?

R: MySpace seems a lot harder to use because the stuff is all over the place and nothing really explains. Facebook everything is detailed.

While this paper concentrates on the Facebook experience, there is little to indicate in the privacy policies or other terms of the main social networking sites that there is any vastly different business model in place. In brief, all of these sites solicit users to post personal information on profiles that they make available either to all or some members of the website. In addition, these services link that information to the actions of their members on the site (and in Facebook's case, with its Beacon service, to actions their users take across the web) and sell advertising based on this profiling and targeting to third party advertisers.

Example: Facebook

Launched in February 2004, Facebook is an online social networking website, describing itself as “a social utility that connects people with friends and others who work, study and live around them.”²⁵ Facebook is a free web-based tool that allows members to customize their profile page to show their birthday, school, political and religious views, relationship status, interests, book, music, tv and movie preferences, schools and work information. The user’s profile can be viewed by all Facebook users unless the user changes their privacy settings to restrict their profile display to their network or friends. Facebook also encourages members to share information with their friends and networks through a number of applications: users can upload photos and tag their friends, publish notes, post videos, create and join groups and events, share links, and update their status. Users can comment publicly on their friends’ “wall”, individual photos and notes or they can converse privately by message or Facebook chat. Members can also add a variety of Facebook applications on their profile, such as games to play with their friends or news on a particular subject. On a user’s homepage, Facebook displays a “news feed”, which aggregates a user’s friends latest activities such as new friends added, wall posts and comments, status and relationship updates and groups and events joined.

Facebook now has more than 90 million active users as of August 2008 and is the fourth most trafficked website in the world.²⁶ According to comScore, Facebook is the number one photo sharing application in the world with more than 24 million photos uploaded daily. Canada is the third largest country on Facebook with more than 7 million active users and with a 30% saturation rate.²⁷ The Toronto network has over 1.2 million members.²⁸

Children on Facebook

Facebook restricts registration to individuals who are 13 years of age or older. In addition, users who are under 18 and not in high school or college are prohibited from using Facebook. Their use is “unauthorized, unlicensed and in violation of these Terms of Use.”²⁹ In the Terms of Use, Facebook states that “By using the Service or the Site, you represent and warrant that you are 13 or older and in high school or college, or else that you are 18 or older, and that you agree to and to abide by all of the terms and conditions of this Agreement.”³⁰ Under Facebook Safety, Facebook advises that “parents of children 13 years and older should

²⁵ <http://www.facebook.com/about.php>

²⁶ Facebook classifies “active users” as those who returned to the site in the last 30 days.

²⁷ <http://www.facebook.com/press.php#/press/info.php?statistics=>

²⁷ <http://www.insidefacebook.com/2008/07/29/tracking-facebook-2008-international-growth-by-country/>

²⁸ As of 21 August 2008.

²⁹ <http://www.facebook.com/terms.php>

³⁰ <http://www.facebook.com/terms.php>

consider whether their child should be supervised during the child's use of the Facebook site."³¹

Despite Facebook's age eligibility restrictions, nearly a quarter of children between the ages of eight and twelve may be using social networking sites such as Facebook, Bebo and MySpace. A poll commissioned by Garlik in the UK suggested that more than 750,000 children in the U.K. are using social networking websites.³² No similar poll has been conducted in Canada, though most of the younger participants (11-13) in our focus group discussions indicated either that they used Facebook or that their friends do.³³ Further research into actual use of social networking sites by children under 18 and especially under 13 in Canada should therefore be a priority, as the limited available data may indicate widespread use of these sites despite nominal legal and contractual restrictions.

Personal Information that Facebook Collects and Shares

Facebook is another example of a website that collects personal information to have a full experience of the site. When a user registers with Facebook, Facebook requests the person's full name, email address and date of birth. As stated above, Facebook also collects various pieces of personal information, such as gender, hometown, political and religious views, instant messaging screen names, telephone numbers, address, relationship status, schools attended, current and previous employers, personal interests and preferences. As well, Facebook collects users' browser types and IP addresses.³⁴ Facebook also states that they may "collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service ... in order to provide you with more useful information and a more personalized experience."³⁵

Facebook's main purpose is to facilitate online social networking, which is clear to the user upon registration and reiterated in Facebook's Privacy Policy and Terms of Use (see Appendix 3 for Facebook's Privacy Policy). Social networking involves sharing photos, messages and other personal information. However, the breadth and scope of what is shared is not clear.

In a complaint to the Privacy Commissioner of Canada filed on May 30, 2008, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) argues that Facebook violates Canadian privacy law (the *Personal Information Protection*

³¹ <http://www.facebook.com/help.php?safety>

³² John Carvel, "Facebook: Children evade social websites' age limits" The Guardian (7 August 2008), online: <http://www.guardian.co.uk/technology/2008/aug/07/socialnetworking.facebook>.

³³ Environics Report, p. 3 and pp. 17-19.

³⁴ Facebook privacy policy

³⁵ Facebook privacy policy

and *Electronic Documents Act* (PIPEDA) on numerous grounds.³⁶ CIPPIC suggests that Facebook violates Principle 4.3.3. by failing to identify its purpose for collecting personal information beyond user names and e-mail addresses. In addition, Facebook violates Principle 4.3.4 by failing to obtain express consent to share users' sensitive personal information. CIPPIC's complaint charges that: "unless users take action to 'opt in' to sharing their sensitive information, Facebook cannot assume consent. As well, Facebook fails to notify users of the uses and disclosures of their personal information." The complaint also charges that the consent Facebook assumes of its users is not valid as the users do not have a full picture of what Facebook does with their personal information (largely marketing):

Facebook does not make a reasonable effort to advise Users of the purposes for which their personal information is used. Facebook also does not advise Users of the extent of their personal information that will be shared by joining a Network. Without this knowledge, Users cannot provide meaningful consent. Instead, consent should be achieved through an opt-in box in the privacy settings. Users can be directed to their privacy settings immediately after completing step 3 of the registration process. Users would then "opt-into" joining a Network, only after confirming that they understood the extent of their personal information that would be shared with Networks.³⁷

Facebook's Business Model

Like Neopets, Facebook uses targeted third party banner advertising. Its business model is also heavily reliant on targeted behavioural marketing. In August 2006, Microsoft struck a three-year deal with Facebook to be the exclusive seller and provider of banner advertising and sponsored links for Facebook.³⁸ Microsoft links advertisers with Facebook members by using "graphical ad placements as well as automated text-based advertisements targeted to content, and over time, aggregate user behaviour on an anonymous basis."³⁹

In October of 2007, Facebook and Microsoft announced that they would expand advertising to cover international markets and Microsoft took a \$240 million equity stake in Facebook.⁴⁰

In November 2007, Facebook launched Facebook Ads, featuring Pages and Social Ads. Through Pages, businesses can create their own interactive profile

³⁶ CIPPIC complaint is available online at: http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf (CIPPIC Complaint). PIPEDA is discussed in more detail, below.

³⁷ CIPPIC complaint at p. 13.

³⁸ <http://www.nytimes.com/2006/08/23/technology/23soft.html>

³⁹ *Ibid.*

⁴⁰ <http://www.facebook.com/press/releases.php?p=8084>

on Facebook to engage customers or fans.⁴¹ Social Ads “allow businesses to become part of people’s daily conversations” by creating an ad that can be targeted to a desired audience by age, location, gender, interests and more.⁴² There are two types of social ads: third party advertising banners located in the ad space to the left of user profiles, and Beacon. Businesses can purchase banner advertising by either number of clicks or impressions. Facebook provides the business with performance metrics, including comprehensive demographic data.

The second type of social ad, Facebook Beacon, is more controversial. Beacon allows businesses to broadcast actions taken by a user to their Facebook news feeds: “social stories, such as a friend’s becoming a fan of [a business’s] Facebook Page or a friend’s taking an action on [the business’s] website, make [the] ad more interesting and more relevant.”⁴³ Beacon actions include purchasing of a product, signing up for a service and adding an item to a wish list. At its launch in November 2007, Facebook announced that 44 websites were using Beacon “to allow users to share information from other websites for distribution with their friends on Facebook.”⁴⁴ Facebook users protested against the Beacon’s release, with nearly 70,000 users signing an online petition calling on Facebook to stop broadcasting users’ transactions without their consent, many particularly upset as Beacon ruined the surprise of Christmas gifts.⁴⁵ MoveOn considered Beacon to be a “glaring violation of [Facebook] users’ privacy by imposing an opt-out regime instead of an opt-in system.”⁴⁶ In December 2007, Facebook made Beacon an affirmative opt-in program and added a privacy control that allowed users to turn off Beacon completely.

Privacy Concerns with Facebook’s Business Model

In its complaint, CIPPIC argues that Facebook’s advertising practices violate PIPEDA in four ways. First, Facebook violates PIPEDA Principle 4.3.2 by failing to notify users of its use of personal information for advertising purposes. Facebook’s Privacy Policy states that Facebook may use information in users’ profiles without identifying the user to third parties. Facebook aggregates user profile information about user preferences to target personalized advertisements and promotions to its users. Advertisements that appear on Facebook are

⁴¹ Facebook Pages, <http://www.facebook.com/business/?pages>

⁴² <http://www.facebook.com/business/?socialads>

⁴³ See <http://www.facebook.com/business/?beacon> and <http://www.facebook.com/beacon/faq.php>

⁴⁴ <http://www.facebook.com/press/releases.php?p=9166>. Some participating websites were eBay, Fandango, CollegeHumor, iWon, echomusic, Blockbuster, Bluefly.com, Joost, LiveJournal, Live Nation, National Basketball Association, NYTimes.com, Sony Online Entertainment LLC, Sony Pictures, TripAdvisor, TypePad, and WeddingChannel.com

⁴⁵ Roy Mark, “Facebook Users Light a Beacon of Protest” eWeek.com (November 21, 2007). Online: <http://www.eweek.com/c/a/Messaging-and-Collaboration/Facebook-Users-Light-a-Beacon-of-Protest/>

⁴⁶ Caroline McCarthy, “MoveOn.org takes on Facebook's 'Beacon' ads” CNET News (November 20, 2007). Online: http://news.cnet.com/8301-13577_3-9821170-36.html

served directly to users by third party advertisers. Third party advertisers receive the user's IP address and "may download cookies to the user's computer or use other technologies such as JavaScript or 'web beacons' ... to measure the effectiveness of their ads and to personalize advertising content."⁴⁷ However, "Facebook does not make a reasonable effort to ensure that Users are advised that their personal information is used for Social Ads" as the default setting includes users in Social Ads.⁴⁸ Because consent is opt-out only, notice is especially important and Facebook's Privacy Policy fails to make clear that personal information is used for the purpose of Social Ads. Children who use Facebook are not likely to understand the complicated wording of the Privacy Policy and may be unaware of the potential dangers of sharing personal information. With the length of the Privacy Policy, most users will likely not read the clause that indicates that personal information is used for the purpose of Social Ads.

There have been suggestions that Facebook collects information without fully disclosing this fact to their members. In December 2007, Computer Associates Security Advisor Stefan Berteau blogged that Facebook misrepresented Beacon to its users, suggesting that Facebook collects information about its users actions on affiliate sites regardless of whether or not the user chose to opt out.⁴⁹ In his experiment, Berteau found that even after logging out of Facebook, information about his online activities linked to his Facebook account name was reported back to Facebook.⁵⁰ Facebook's Beacon FAQ statement that "Facebook affiliates communicate with Facebook only if a user is logged into their account" conflicts with Berteau's findings.

Second, CIPPIC argued that Facebook violated PIPEDA Principle 4.3.3 by conditioning its service on users' consent to sharing their personal information for the purpose of Social Ads. Facebook's members are required to agree to the use of their personal information for the purpose of displaying advertisements on Facebook.

Third, CIPPIC argued that Facebook violates PIPEDA Principle 4.3.6 by failing to seek express consent from users to share their sensitive information. Users are likely to post several pieces of sensitive information on their profile. As an example, CIPPIC suggests that "the fact that a User is female, 13 years old, lives in a small town and attends a certain school is likely sensitive information."⁵¹ Users consent to the use of their personal information for advertisement by

⁴⁷ Facebook Privacy Policy; see Appendix 3.

⁴⁸ CIPPIC Complaint, p. 16.

⁴⁹ "Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in" CA (3 December 2007), online: <http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx>.

⁵⁰ See also "Facebook's Beacon More Intrusive Than Previously Thought" PC World (30 November 2007), <http://www.pcworld.com/article/id,140182-c.onlineprivacy/article.html>.

⁵¹ CIPPIC complaint at p. 17.

agreeing to Facebook's Privacy Policy and sensitive personal information is treated the same as all personal information, meaning that it may be used by Facebook without a user's express consent.

Finally, CIPPIC charged that Facebook violates PIPEDA Principle 4.3.8 by not allowing users to withdraw consent to using their personal information for advertising purposes. Facebook only allows users to opt out and withdraw consent from Beacon and Social Ads in the news feed, users cannot opt out or withdraw consent from targeted banner advertisement displayed on Facebook's Ad Space.

Facebook's business model is predicated on a sophisticated system of personal information collection and data sharing with affiliate advertisers. Third party advertisements and Facebook features such as Social Ads and Beacon are not explained well by Facebook's Privacy Policy, which is long and difficult to understand.⁵² In such a situation, it is dubious that children can consent in an informed manner to Facebook's proposed collection, use and disclosure of their personal information. Given the indications that children under 13 are using Facebook and other social networking sites like Facebook, the concern with relying solely upon consent based on a complex and lengthy privacy policy increases.

Yet, even if Facebook rewrote their privacy practices to address the failures alleged by CIPPIC, their marketing practices might still be inappropriate for users that are under the age of 13 and for teenage users between the ages of 13 and the age of majority. This is because the social science research indicates that children and teens view privacy less abstractly than adults and place it resolutely in the context of their social relationships.

In an article criticizing Facebook's Beacon, Professor Valerie Steeves argued that data protection focuses on narrow procedural rights over information, failing to account for the way young people actually use social networking sites:

Even though the information may be available to others and be innocuous in and of itself, Facebook's actions side-stepped the careful presentation of the self that young people enact in online media. Accordingly, young people are unable to trade away their privacy in exchange for the advantages of social networking, in spite of the legalities of the site's user agreement, because privacy is central to the way they construct their identities and negotiate their social relationships.⁵³

⁵² Facebook's Privacy Policy is reproduced in Appendix 3 and runs to 7 pages in 10 point type.

⁵³ Valerie Steeves, "Data Protection Versus Privacy: Lessons from Facebook's Beacon". In press. In D. Matheson, ed., *The Contours of Privacy*. (Newcastle upon Tyne, UK: Cambridge Scholars Publishing) at p. 4.

In other words, since friendship creation, social interaction and identity creation are at the heart of children's and especially teens' emotional and mental development, they are simply unable to separate self from social world to the extent necessary to satisfy the "privacy bargain" in social networking. Teens cannot fathom trading collection use and disclosure of personal information to a third party (for marketing or any non-social networking purpose) for the opportunity to participate in this new social environment. Steeves suggests children and teens simply could not "consent" to this bargain even if they were aware of the "privacy bargain": they still will feel their privacy is violated when the stated use is actually made of the information.

The teens in our focus groups said that if they could set privacy options, they would no longer worry about privacy:

R: *First of all in the contract for I think all of them, if you don't accept, they don't allow you to make an account. (11-13 year old)*

M: That's a good point. So my question is, is it worth it to give up a little bit of your privacy?

R: *Well on Facebook, yes cause you do bring it back. There's a whole section about privacy but for like websites where you can't change any privacy, anybody can just walk in and look at your picture, then it's not worth it. But if you can choose the privacy, it is. (11-13 year old)*

This type of answer may indicate some children, especially at the early teen stage, conceptualize privacy in relation to the standard biographic information they have been told not to freely give to another live person. In this case, any statements in a corporate privacy policy about using other personal information, either in the aggregate or to profile an individual user, would appear to be confused by this age group with privacy settings on the website for personal biographic information. However, more research on this concept of privacy should be done to investigate if children of this age do in fact conflate the concept of data aggregation and profiling with the information that can be controlled via the registration or "privacy" settings of social networking sites.

Our focus group participants explained that amongst social networking sites they trusted Facebook more than other social networking sites and felt it was more privacy secure than others. :

R: *Safety? Just not giving out too much personal information like I use Vibe⁵⁴ but I don't give out too much information and in Facebook and stuff*

⁵⁴ Vibe.to was one of the social networking sites visited by a focus group participant. Focussing on the Toronto area, it does allow profiles to be displayed by general visitors to the site without registering. In addition, the site has a tool on its home page allowing the casual Internet browser to select gender, age range and general location information. The age range is 14-99 years old. A more detailed search page is

like that. On Facebook it's pretty safe because people can't go on your profile unless you accept them as a friend so it's safe. (14-17 year olds)

As noted in the CIPPIC complaint, and on reading the Facebook Privacy Policy, the above statement is potentially wrong. “Strangers” who are not friends or in a network of the user can see another user’s profile unless that user goes into their privacy settings and selects this restriction. This may indicate a general lack of awareness of the true content of the privacy policy and again may point to a confusion on the part of child and teenaged Facebook users that the presence of privacy tools indicates that they have been set to their strictest “most private” setting.⁵⁵ More research on this possible tendency is indicated – given that the perception leaves these teens open to the exact privacy violations they feel they are avoiding by using the service.

Risks of Overcollection of Data and Profiling to Children

As stated by the National Consumers League, “profiling for advertising purposes raises serious concerns about privacy, security, discrimination, and use for secondary purposes such as law enforcement.”⁵⁶

Collection of profile information on children, in addition to the developmental concerns of the social science research community detailed above, also raises the possibility of misuse of that information either by those who collect and share it in the present marketing context or by other third parties who may obtain access to these records via exceptions to privacy requirements for investigation of crimes or for civil litigation. Some of these potential misuses include:

- Use the information to target individuals with specific advertising based on stereotypes based on their personal characteristics (age, sex, race, religion, ethnicity).
- Use the information to price discriminate against individuals, and

also available on the results page if one clicks on “more members” that lets the user specify more details such as country, marital status, eye colour, hair colour and whether the profile subject has posted pictures. A search performed in mid-August 2008 by PIAC returned 132 profiles for “females” “14-17” in “Markham”.

⁵⁵ It may be that teens or children are not any less perceptive than adults in this area. Note that a U.S. study concluded that 63% of American adults wrongly concluded that the mere presence of a privacy policy meant that the website could not collect personal information about them. See Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace, Joseph Turow, Deidre K. Mulligan, Chris Jay Hoofnagle, University of Pennsylvania Annenberg School for Communications and UC Berkeley Law’s Samuelson Law, Technology & Public Policy Clinic, October 2007, http://www.law.berkeley.edu/clinics/samuelson/annenberg_samuelson_advertising-11.pdf at p. 3.

⁵⁶ See Testimony of Leslie Harris of the Center for Democracy and Technology before the U.S. Senate Commerce, Science and Transportation Committee, July 9, 2008. Online: http://www.nclnet.org/privacy/comments_FTC_behavioral_marketing_11162007.pdf (Harris Testimony).

- Access by Governmental agencies for law enforcement, security, child welfare and intelligence purposes.
- Access by schools and individuals in defamation lawsuits or other lawsuits and by media rights holders to assist in civil copyright actions.

While the spectre of law enforcement access to personal information seems farfetched, recall that nearly every privacy policy claims the discretion to comply with law enforcement requests for such information. For example, the Facebook Privacy Policy (see Appendix 3) contains the following statement:

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.

It is unclear on this wording if Facebook would require a warrant to release personal information of minors in relation to law enforcement or in civil litigation, a court order to produce the information.

Yet, the possibility of access to sensitive personal information does exist. One participant in the focus groups visited Facebook and left a comment on a friend's page to the effect of "liked your work on Jarvis". From observing this participant and the clicktrail of other sites visited, it was apparent the teen (11-13) was a graffiti artist. The online profile of this individual possibly would lead to discovery of pictures of his or her graffiti style or "tag" – the equivalent to finding a graffiti artist's "black book" of graffiti style – and be perfect evidence for police looking to prosecute graffiti artists or to companies looking for reparation of defacement of their property.

This very risk was highlighted in a recent European Union Article 29 Working Party (Privacy) document that discussed the limits of what information created a "means to identify" a person and therefore should be considered personal information and protected under European privacy laws. It gave the following example in relation to graffiti:

Example No. 16: damage caused by graffiti

Passenger vehicles owned by a transportation company suffer repeated damage when they are dirtied with graffiti. In order to evaluate the damage and to facilitate the exercise of legal claims against their authors, the company organizes a register containing information about the

circumstances of the damage, as well as images of the damaged items and of the "tags" or "signature" of the author. At the moment of entering the information into the register, the authors of the damage are not known nor to whom the "signature" corresponds. It may well happen that it will never be known. However, the purpose of the processing is precisely to identify individuals to whom the information relates as the authors of the damage, so as to be able to exercise legal claims against them. Such processing makes sense if the data controller expects as "reasonably likely" that there will one day be means to identify the individual. The information contained in the pictures should be considered as relating to "identifiable" individuals, the information in the register as "personal data", and the processing should be subject to the data protection rules, which allow such processing as legitimate under certain circumstances and subject to certain safeguards.⁵⁷ [Emphasis added.]

Furthermore, by obtaining an online profile of individuals from a young age, companies can target them with advertising and products specific not only to their perceived characteristics but also to their present and future stage of personal development on the road to adulthood. Given the prevalence of ads served to teenagers that are for age-inappropriate items such as dating services and nightclubs,⁵⁸ there is a distinct possibility of profiling of "what type of adult this teen will be". Research is therefore required to explore if, for example, online profiling of teens (for example a preference for chance based online games) will be used to lead them to adult problems, such as online gambling.

Personal information of an individual may determine that they are from a wealthy income bracket, then it can begin to sell products to that individual at a higher price than it would to others.⁵⁹ Conversely, lower income individuals may be "redlined" that is, identified as a marginalized group that is offered poorer terms than more "mainstream" populations, for example, those identified as coming from such vulnerable populations may be marketed subprime credit products.⁶⁰

Since it is difficult to determine, due to lack of disclosure from online marketers, if this actually is happening, or if it is, to what extent and how, more research

⁵⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY in WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June, online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf at p. 17.

⁵⁸ See "fair game?" *supra*, at p. . During our focus groups one participant (14-17) using Vibe.to was served an ad for a service rating Canadian nightclubs.

⁵⁹ See L. Story, "Online Pitches Made Just for You" New York Times (March 6, 2008). Online: <http://www.nytimes.com/2008/03/06/business/media/06adco.html> This story is quoted for proof of the potential of differential pricing by Leslie Harris of the Center for Democracy and Technology

⁶⁰ See COMMENTS OF DR. MARK COOPER, DIRECTOR OF RESEARCH, CONSUMER FEDERATION OF AMERICA TO THE FEDERAL TRADE COMMISSION TOWN HALL MEETING ON "EHAVIORAL ADVERTISING: TRACKING, TARGETING AND TECHNOLOGY" November 16, 2007 at p. 3. Online: http://www.consumerfed.org/pdfs/Mark_Cooper_Comments_Ehavioral_Advertising_11-16-07.pdf

specifically on behavioural marketing should be done, particularly in the period of transition as kids become adults.

Criticisms of Behavioural Marketing to Children

Numerous academics and reports all have panned the growth of immersive marketing environments and children's websites and services that rely upon extensive collection, use and disclosure of children's personal information.⁶¹

These criticisms are based on objections relating to child development, child protection, what is marketed, and privacy concerns.

Susan Linn, a sociologist, makes the argument in her book *Consuming Kids: The Hostile Takeover of Childhood*, on all these bases but focuses on child development and argues that such immersive advertising environments are detrimental to the child's own development by invading the child's sense of how to play – potentially emotionally and mentally impoverishing the child.⁶²

According to Professor Valerie Steeves, “corporations seeking to capitalize on this market create websites that offer games, quizzes, chat environments and advice in order to encourage children to provide their personal information, which can then be used to target the children with advertising.”⁶³ The result of this activity is surveillance, and this surveillance is an assault on democratic thinking in the child – potentially reducing the next generation to “brand sheep”.

These sites mine children's play and communication to manipulate their social relationships and sense of self, embedding their brand into the child's private life. I argue that this constitutes a profound invasion of children's online privacy, and significantly restricts the potential of the Internet to play a constructive role in children's lives.⁶⁴

Jeff Chester and Kathryn Montgomery have pointed out that children are now facing not only behavioural profiling and targeted marketing, but also the commercialization of online communities, brand-saturated online environments, viral video advertising and advertising through avatars.⁶⁵ Their main concern is

⁶¹ See Steeves, “Not Child's Play”, *supra*, Center for Media Education, *Web of Deception: Threats to Children from Online Marketing* (Washington, DC: 1996); Kathryn Montgomery, *teensites.com* (Washington, DC: Center for Media Education, 2002), Susan Linn, *Consuming Kids: The Hostile Takeover of Childhood* (New York: The New Press, 2004) (Consuming Kids).

⁶² See Linn, *Consuming Kids*, ch. 4 “Endangered Species: Play and Creativity”.

⁶³ “Not Child's Play” at p. 174.

⁶⁴ See Valerie Steeves, “The Watched Child: Surveillance in Three Online Playgrounds”

⁶⁵ Jeff Chester and Kathryn Montgomery, “Interactive Food and Beverage Marketing” (Berkeley: Berkeley Media Studies Group, May 2007), at pp. 34-52. Online:

<http://digitalads.org/documents/digiMarketingFull.pdf>

marketing of fattening, unsafe or age-inappropriate products and services to youth.

The conclusion that much of the advertising that is paying for behavioural marketing is for products that are poor nutritional choices or are flatly inappropriate for teens and children (as selling the products is restricted by law to adults) was also made in the “Fair Game?” report of the U.K. National Consumers Council. It found that of 70 advertisements displayed on children’s websites, 9% were for online gambling, 6% for credit or loans, 4% for online dating, 3% for elective (eye) surgery, and 3% for car insurance.⁶⁶ While there may be regional differences to account for the high gambling percentage, and the sample size is small, this tendency to age-inappropriate content (25% of all ads) merits close examination in the Canadian context.

Finally, children’s privacy in relation to these interactive playgrounds has been cited by Valerie Steeves and the U.K. National Consumers Council as based upon “pervasive registration” and constant tracking,⁶⁷ in essence, creating a surveillance system. Steeves argues that the mere existence of surveillance of this nature is destructive of socially-created and negotiated privacy, and therefore interfere’s with children’s identity and social relationships:

Once the broad-ranging impact of invasive marketing techniques on the development of a child’s identity and social relationships is brought into the privacy debate, it becomes much easier to conclude that that form of surveillance is not socially appropriate. It is no longer a question of tinkering with process, but of coming to social judgment about substance. Current pressures to strip the veil of online anonymity and authenticate the identity of users are rooted in the desire to promote efficiency and security. However, the questions around children’s online privacy remind us that there is value in maintaining infrastructures that allow for anonymous interaction.⁶⁸

Given the possible risks, and overwhelmingly negative reaction of social scientists to business models based on collection of children’s information online, it is necessary to understand what controls presently exist in this area.

⁶⁶ See “Fair Game?”, *supra*, at p. 14.

⁶⁷ See Steeves, “Not Child’s Play” at p., and “Fair Game?” at p 27: “Overall, 38 of the 70 companies behind the advertisements we examined requested personal details (54 per cent). About half asked for an email address and name; roughly a third requested a date of birth or age, address and postcode; and more than 10 per cent required landline and/or mobile telephone numbers.”

⁶⁸ Steeves, “Not Child’s Play” at p. 187.

Children's Privacy Online - The Legal Context

Although not legal standards, voluntary codes of advertisers towards marketing to children have existed for at least 20 years in Canada. These thus predate much of Canada's privacy legislation and continue to this day. In addition to privacy laws and industry codes, there as well have been recent initiatives by the Federal and provincial privacy commissioners to address children's online privacy, somewhat indirectly however, so far. We examine these controls in turn.

Voluntary Ad Industry Standards

Canadian Standards

Various initiatives within the advertising industry have created voluntary codes of conduct to self-regulate advertising practices. These voluntary codes attempt to address special standards and practices for marketing to children, but speak generally and often fail to address children's use of online playgrounds and social networking websites.

In Canada, the Canadian Marketing Association (CMA) is the largest marketing association, representing over 800 corporate members. The CMA's Code of Ethics and Standards of Practice ("Code of Ethics") is compulsory for members, which establishes and maintains high standards of practice that are a "fundamental responsibility to the public, essential to winning and holding consumer confidence, and the foundation of a successful and independent marketing industry in Canada."⁶⁹ The Code of Ethics requires consumer marketers to abide by the ten privacy principles in PIPEDA.⁷⁰

The CMA Code of Ethics stipulates special considerations for marketing to children and teenagers. A "child" refers to somebody who is younger than 13 years old, whereas a "teenager" refers to somebody who is older than 13 years of age but has not reached the age of majority in their province or territory of residence.

For marketing to children (under 13 years), the Code of Ethics requires that "all marketing interactions directed to children that include the collection, transfer and requests for personal information require the opt-in consent of the child's parent or guardian." Where the child, parent or guardian withdraws or declines

⁶⁹ <http://www.the-cma.org/?WCE=C=47|K=225849> – Purpose of CMA Code of Ethics and Standards of Practice

⁷⁰ CMA Code of Ethics – section J.

permission to collect, use or disclose a child’s information, marketers must immediately delete all such information from their database.⁷¹ Additionally, marketers must not knowingly accept an order from a child without a parent or guardian’s opt-in consent and are not allowed to pressure a child to urge their parents to purchase a product or service.⁷²

For teenagers between the ages of 13 and 16, marketers must obtain opt-in consent from the teenager for the collection and use of their “contact information”.⁷³ Prior to disclosing their contact information, marketers must obtain the opt-in consent of their parent or guardian. For the collection, use or disclosure of personal information that exceeds contact information belonging to a teenager of this age category, the opt-in consent of their parent or guardian must be obtained.⁷⁴ For teenagers over the age of 16 but below the age of majority, marketers must obtain the teenager’s opt-in consent for the collection, use and disclosure of their personal information.⁷⁵ However, where the teenager, parent or guardian withdraws or declines permission to collect, use or disclose a teenager’s personal information, the marketer must immediately delete all such information from their database.⁷⁶

Summary of Consent Provisions for Marketing to Children and Teenagers

Age	Type of Information	Opt-in Consent Requirement
Under 13	Any personal information	Parent or guardian
13, 14 and 15	Contact information only	Teenager
13, 14 and 15	Personal information beyond contact information	Teenager <u>and</u> parent or guardian
16 and over	Any personal information	Teenager*

*Note: As per Section L3.3 of this Code, a parent or guardian can withdraw consent to use or disclose personal information for teenagers of all ages, including 16 years of age and over.⁷⁷

Additionally, the Code of Ethics warns marketers that transactions with teenagers may not be legally enforceable against the teenager or his parent or guardian.⁷⁸

Notably, the CMA Code of Ethics prohibits marketers from “unduly [exploiting] teenagers’ impressionability, or susceptibility to peer or social pressures.”⁷⁹

⁷¹ CMA Code of Ethics – K3.1 and K3.2

⁷² CMA Code of Ethics – K7

⁷³ “Contact Information” is defined in the Glossary of Terms in the Code as: “A subset of personal information, contact information refers solely to an individual’s name, home address, e-mail address and/or telephone numbers. This subset of personal information is considered non-sensitive.” This corresponds roughly to the idea of “personally identifiable information (PII) discussed below in terms of U.S. law.

⁷⁴ CMA Code of Ethics – L3.1

⁷⁵ CMA Code of Ethics – L3.2

⁷⁶ CMA Code of Ethics – L3.3

⁷⁷ Chart from CMA Code of Ethics, at L.3.3

⁷⁸ CMA Code of Ethics – L7. There is a similar sections regarding children (under 13), see .K2, K3 and K5.

⁷⁹ CMA Code of Ethics – L5

However, the Code of Ethics is meant to be general and does not specifically address challenges of modern online behavioural marketing strategies and how children use the internet. Although the CMA is considering how to advise its members in relation to behavioural marketing, it appears that guidance from the Association is some way off.⁸⁰

Nonetheless, it is noteworthy that the CMA Code addresses children differently considering their age and presumed maturity and tailors its privacy requirements to that maturity level. It is also noteworthy in requiring opt-in (explicit) consent for most collection, uses and disclosures of personal information (of any kind) and also gives a parental control veto over disclosure of personal information of all children under 16. Finally, its explicit recognition of children as a vulnerable population that must not be exploited by marketing is exemplary.

Finally, Industry Canada organized a working group of stakeholders including government, business and consumer groups and developed the Canadian Code of Practice for Consumer Protection in Electronic Commerce in 2004. Endorsed by the Federal-Provincial Consumer Measures Committee, this document does deal with children's privacy online, however, it does not specify age limits. The Code states, in relation to children's privacy:

Principle 8: Communications with Children

8.1 All vendors have a social responsibility to determine whether the person with whom they are communicating or transacting is a child. When communicating with children, or when the content is likely to be of interest to children, the language must be age-appropriate, must not exploit the credulity, lack of experience or sense of loyalty of children, and must not exert any pressure on children to urge their parents or guardians to purchase goods or services.

8.2 Vendors shall take all reasonable steps to prevent monetary transactions with children.

8.3 Vendors shall not collect, use or disclose personal information of children without the express, verifiable consent of their parents or guardians, except as provided for in 8.5 and 8.6 below. When seeking parental consent, vendors shall clearly specify the nature of the proposed

⁸⁰ The CMA has confirmed with PIAC that it is considering behavioural marketing: "Unfortunately we do not have any CMA studies pertaining to behavioral marketing. It is certainly a very current topic of interest within the marketing community and beyond, and the Association is considering the issue. Whether it would be in the context of our Code of Ethics, best practices guidelines or a "white paper" on the subject to better educate member companies, we will be determining how we can help CMA members ensure that they remain on a sound ethical and legal footing as they engage in behavioral marketing." E-mail from Wally Hill, Vice President, Public Affairs & Communication, Canadian Marketing Association to PIAC researcher, Wednesday, June 25, 2008 3:57 PM.

communications, the personal information being collected and all potential uses of the information. [Emphasis added.]

8.4 Vendors shall not knowingly send marketing e-mail to children.

8.5 When contests or clubs are directed at children, vendors may collect children's personal information without parental consent and communicate directly with those children, when vendors:

- a) collect the minimum amount of information required to provide the club membership or to determine the winner of a contest;
- b) limit communications only to those required to provide the club membership;
- c) in the case of contests, only deal with the parents or guardians of the winner(s) and do not contact the winner(s);
- d) retain the information only as long as the children remain members of the club or until the conclusion of the contest; and
- e) make no use of the information other than to provide the club membership or to determine a contest winner.

8.6 When vendors contract with third parties to provide a club membership or to determine the winner of a contest, vendors shall disclose only the personal information necessary for this, and shall ensure that the third parties agree to comply with principles 4 and 8.

It is notable that this Code prohibits collection, use or disclosure of "children's" personal information unless there is express, verifiable parental consent. Unfortunately, as pointed out by CIPPIC, these principles are voluntary and not all Canadian online businesses follow them.⁸¹

U.S. Standards

In the United States, the Network Advertising Initiative (NAI) is a cooperative of online marketing companies "committed to building consumer awareness and establishing responsible business and data management practices and standards."⁸² The NAI recently announced a draft self-regulatory Code of Conduct for Online Behavioural Advertising (draft NAI Code of Conduct).⁸³ The draft NAI Code of Conduct recognizes the advance of new advertising solutions and business models for third party advertising on the Internet.

⁸¹ CIPPIC, "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Act ("PIPEDA")" (November 28, 2006) at p. 15. Online:

http://www.cippic.ca/documents/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf

⁸² <http://networkadvertising.org/about/>

⁸³ http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf

The draft NAI terms “online behavioural advertising” to mean “any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online.”⁸⁴ The draft NAI Code of Conduct stipulates fair information practices for “personally identifiable information” such as transparency, notice, choice, use limitation, transfer and service restrictions, access, reliability and security.⁸⁵ NAI members are required to maintain a website to offer explanations of online behavioural advertising and information about and centralized access to consumer choice mechanisms.⁸⁶ As well, each member is required to post “clear and conspicuous” notice describing their data collection and use practices on their website.⁸⁷ Consumer choice is also a priority, requiring a consumer opt-out mechanism for the use of non-personally identifiable information.⁸⁸

The draft NAI Code of Conduct prohibits the use of non-personally identifiable information or personally identifiable information to create an online behavioural advertising segment that specifically targets children under the age of 13.⁸⁹ However, this protection for children is not as comprehensive as the CMA Code of Ethics, which also considers “teenagers” between the age of 13 and the age of majority and provides for special rules.

The draft NAI Code of Conduct covers online behavioural advertising, such as the standard process of collecting information about a particular user’s surfing habits to deliver targeted third-party advertising to a specific individual. However, new business models for online marketing such as Neopets’ “immersive advertising” through stealth product placement and the fact that the third party does not see (for the most part) the child’s profile (Neopets does) and Facebook’s Social Ads are simply not contemplated within the draft NAI Code of Conduct. Instead, the draft NAI Code of Conduct deals solely with the standard third party marketing business model and not the models used in social networking sites and immersive playsite environments that children use. The draft NAI Code of Conduct does not address children’s behavioural marketing except those under 13. Thus, the draft NAI Code of Conduct appears to miss a chance to take these new business models into account and to regulate the potential abuses identified above in relation to online behavioural marketing targeted to children under 18.

⁸⁴ Draft NAI Code of Conduct – II.1.

⁸⁵ Draft NAI Code of Conduct – III.

⁸⁶ Draft NAI Code of Conduct – III.1

⁸⁷ Draft NAI Code of Conduct – III.2.a

⁸⁸ Draft NAI Code of Conduct – III.3.a.i.

⁸⁹ Draft NAI Code of Conduct – III.4.a.

Legal Standards – Overview

Canada, at the federal and provincial level, has done little to regulate advertising directly targeting children. The sole exception is the Province of Quebec, which, in its *Consumer Protection Act*, specifically bans advertising directed to children under the age of 13. This prohibition withstood a legal challenge under the Charter of Rights and Freedoms in the leading Supreme Court of Canada case, *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927 (*Irwin Toy*). Other provinces and the federal government have not seen fit to follow this lead in their respective areas of legal jurisdiction.

As a result, the only legal standards that can be said to control behavioural online marketing to children are Canadian privacy laws operating in the marketplace: the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and “substantially similar” provincial statutes. The question therefore remains what sort of legal controls these laws place on collection, use and disclosure of children’s information for the purpose of advertising.

Legal Capacity, Consent and Children in Canada

Part of the complication with protecting children’s privacy is the fact that children are treated in a particular manner by the general law, especially in Canada. This general law context greatly, if invisibly, shapes the approach of privacy law to dealing with children.

In common law provinces, that is, provinces other than Quebec, legal minors (children and teens under 18 years of age) are considered to be under a legal incapacity, such that the law and courts will not protect them without assistance from an adult.⁹⁰ These adults can effectively make important decisions about a child’s legal rights and represent them and their interests in transactions. Parents or “legal guardians” thus make contracts or otherwise exercise the legal rights of children.⁹¹ However, this power to exercise the child’s legal rights does not give the responsible adult (usually, but not always a parent) *carte blanche*, instead, the adult must generally act in the “best interests of the child”.⁹²

⁹⁰ A description of the legal capacity of minors, tutelage and other civil law concepts in Quebec is beyond the scope of this paper.

⁹¹ “Minors” may make contracts for “necessities”, however, this relates to items such as food, shelter and medicine, not online discretionary services. For an excellent description of minors’ rights in contracting, see the description of U.K. law (which is essentially identical to common law in Canada) at: Out-Law.com, User Generated Guides, “Moderation, liability and terms of use” (February 2007). Online: <http://www.out-law.com/page-7841>

⁹² See Grover, Sonia C., *The Child’s Right to Legal Standing* (Markham, Ontario: LexisNexis Canada Inc., 2008) at p. ix. Note that this text paraphrases Martin Guggenheim, *What’s Wrong With Children’s Rights* (Cambridge, Mass: Harvard University Press, 2005) to the effect that “the notions of

Nonetheless, the law in certain aspects does recognize the growing maturity of children and especially late teens as they come closer to this legal adulthood. Thus the law in medical situations involving consent to treatment recognizes the concept of a “mature minor”.⁹³ A mature minor can be any age of child beyond infancy but the law requires a judge to inquire into the relative maturity of the child and his or her understanding of proposed medical intervention (for example a blood transfusion) before deciding if the child is mature enough and understands the procedure adequately to consent to the medical treatment on his or her own.

Medical consent is very close in nature to consent to use of personal information. Both require that the “consent” given, in order to be valid legally, must be “informed”.⁹⁴ Informed consent requires not only that the consent be freely given without coercion, but also that it be fully informed, that is, that the person giving the consent has all the reasonably necessary information about what they are consenting to before consenting. In a medical context, this includes information on both usual risks and complications and additionally, information on any serious risks that may not be likely, but are possible. The question then arises as to whether the law of privacy has advanced to the same stage as medical law, and that since risks associated with poor privacy, such as stalking, identity theft and damage to reputation are now commonplace results of privacy breaches, if these extra risks also should be disclosed to people making the decision whether to release their personal information to a retailer, financial institution, marketer or government department.

With this background regarding general legal incapacity and mature minority in consent situations in Canadian common law provinces, we turn to consideration of Canada’s existing privacy law.

‘best interests of the child’ and ‘children’s rights’ are routinely co-opted to serve adult interests and not those of children.”

⁹³ For an excellent description of the legal concept of a mature minor and consent in the medical context in the U.K. (which law mirrors that of Canada), see the description of “Gillick competence” in Foundation for Information Policy Research, “Children’s Databases – Safety and Privacy: A Report for the Information Commissioner” (London?: FIPR, November 2006), Online: http://www.fipr.org/childrens_databases.pdf . Note that this paper also calls into some question the use of the mature minor consent rule for large scale “blanket” information gathering and posits that the concept of a mature minor may be abused in situations where there is a strong incentive to collection personal information of youth, such as for child welfare databases.

⁹⁴ For medical informed consent see: *Reibl v. Hughes* (1980), 114 D.L.R. (3d) 1 and for privacy see *Englander v. TELUS Inc.*, 2004 FCA 387 at para. 56.

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA and Children

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)⁹⁵ applies to the websites most frequented by Canadian children. It applies to social networking, for example, because these websites accept paid advertising and may sell personal information of users to third party advertisers for targeted or behavioural advertising. Indeed, it appears that the true “value” (in a corporate marketing sense) in the social networking and other sites frequented by children may be less in the direct “banner” advertising and more in third party targeted marketing.

PIPEDA makes no distinction, on its face, between “adults” and children or legal “minors”. The Office of the Privacy Commissioner of Canada (OPCC) has been nearly silent in interpreting this Act in the light of the collection, use and disclosure of information from children, probably due mostly to the fact that the Office is complaint-driven, and not many parents have taken the time to complain on behalf of their minor children. First, the OPCC has issued a Guideline to Business on obtaining consent in commercial transactions and stated simply that: “For an individual who is a minor, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian, or person having power of attorney.”⁹⁶ Secondly, the OPCC recently has created a website for “youth” about privacy (especially on the Internet and on social networking websites (see <http://www.youthprivacy.ca/en/index.html>)). Finally, in a campaign detailing social networking, the OPCC obviously has targeted itself the youth market by placing most of the emphasis on a well-produced flash presentation (video) rather than in long-winded documents.⁹⁷ In essence, therefore, the OPCC has provided little non-binding guidance to use of children’s private information, especially for targeted behavioural marketing, the mainstay of the business models of children’s most popular websites.

⁹⁵ And in the provinces of British Columbia, Alberta and Quebec, substantially similar provincial privacy acts apply. This study has not considered those acts in depth but they are not dissimilar in treatment of personal information of minors.

⁹⁶ See Office of the Privacy Commissioner of Canada, “A Guide for Businesses and Organizations: Your Privacy Responsibilities” (Ottawa: Public Works and Government Services Canada, 2003), <http://www.privcom.gc.ca/information/guide_e.asp> at p. 9.

⁹⁷ See OPCC, “Social Networking and Privacy”, online: http://www.privcom.gc.ca/information/social/index_e.asp and especially the flash presentation at: http://www.privcom.gc.ca/fs-fi/02_05_d_35_sn_e.asp

PIPEDA itself, in its explanatory notes to the Schedule 1, which contains the detail of the ten “privacy principles” of PIPEDA, makes a few more references to children’s privacy. However, these references stress the incapacity at law of children or the ability of parents to consent on behalf of the child in some circumstances.⁹⁸

An important ambiguity in PIPEDA, therefore, is whether the personal information control remains in the hands of the child or a parent or guardian. In other data protection regimes, it is clear that the “data subject,” that is, the person with the right to control data about them, is the person himself or herself that is the subject of the data, whatever their age. This is the case in European Union law,⁹⁹ and U.K. privacy law.¹⁰⁰ The child’s right to data control can be *exercised* by a parent in certain cases, but it remains the right of the child.

This means that under PIPEDA as it to now has now been considered by the OPCC, children’s personal information may possibly be collected under exactly the same rules as that of adults, with the added wrinkle that consent may be that of the parent or guardian, not the child him or herself, largely at the choice of the marketer.

Consent under PIPEDA

The protective mechanism that PIPEDA applies to all personal information collection, use and disclosure therefore is the concept of consent. Section 5, subs. 1, indicates that all organizations “shall comply with the obligations set out in Schedule 1.” Schedule 1 is based on a Canadian Standards Association standard and sets out ten privacy “principles” that organizations must abide by in collecting, using or disclosing personal information in the course of commercial activities. Principle 4.3 of Schedule 1, and its sub-principles, attempts to delimit the scope of consent and what is required to procure it.¹⁰¹ Principle 4.3 states simply:

⁹⁸ See PIPEDA, Schedule 1, Principle 4.3 (Note): “Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.” and Principle 4.3.6, which reads in part: “Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).”

⁹⁹ See EU Article 29 Data Protection Working Party, “Working Document 1/2008 on the protection of children’s personal data (General guidelines and the special case of schools), WP 147, Adopted on 18 February 2008. (Article 29 WP 147) Online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

¹⁰⁰ See Office of the Information Commissioner, “Protecting Children’s Personal Information ICO Issues Paper”, V.1 (London, OIC, 22 November 2006) at p. 7. Online: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_childrens_personal_information.pdf

¹⁰¹ See, generally, See J. Lawford, “CONSUMER PRIVACY UNDER PIPEDA: HOW ARE WE DOING?” (Ottawa: PIAC, 2004) at pp. 15-17. Online: <http://www.piac.ca/files/pipedareviewfinal.pdf> (“PIPEDA: How are we doing?”)

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

As noted above, some confusion enters into the statement in relation to children, as the explanatory note to Principle 4.3, as “Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.” However, it appears implied that someone’s consent is required to process personal information of children, whether that be the child’s or a responsible adult’s. It does not appear that this note completely absolves advertisers from seeking any consent in relation to children’s private information.

PIPEDA unfortunately does not further assist as it does not define what “consent” means for the purpose of the Act. As noted above, however, the Federal Court of Appeal has equated the use of the word “consent” in PIPEDA with the concept of “informed consent” in the general law, most often interpreted in cases involving medical consent to treatment. As detailed above, PIPEDA also does not have any reference to the concept of “mature minor” in relation to a child (teen) consenting to the collection, use or disclosure of his or her personal information. It should be noted in this regard that the European Union law and international law in particular accord much more autonomy of action on the part of a child in the area of privacy law than Canadian law.¹⁰² Even the voluntary Best Practices regarding Marketing to Minors of the Canadian Marketing Association recognizes,¹⁰³ (detailed above – in a reverse way, by permitting more autonomy of decision to older teens), the growing maturity of 16- and 17-year olds versus younger teens and children by having different rules regarding their membership’s interaction with them (and therefore the need to seek consent more directly from these older teens).

Is the Canadian law, therefore, as expressed in PIPEDA and absent clear concepts of consent and legal incapacity/mature minority, adequate to ensure that collection, use and disclosures of personal information from children culled from websites is not a privacy invasion?¹⁰⁴

Professor Val Steeves, a consultant on this project, finds that consent is not an effective legal mechanism to protect privacy of children using the Internet. Her argument is two-fold: first, neither children nor parents read, or if they read, understand, privacy policies of major Internet websites. Readability of these privacy policies is a major impediment to their intelligibility, calling into question if “informed consent” ever could be given by an average child or parent to the

¹⁰² See EU Article 29 Data Protection Working Party, “Working Document 1/2008 on the protection of children’s personal data (General guidelines and the special case of schools), WP 147, Adopted on 18 February 2008. (Article 29 WP 147) Online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

¹⁰³ As well as the guidelines of the U.K. Advertising Standards Authority.

¹⁰⁴ On this point, see Steeves, *It’s Not Child’s Play*, supra, at p. 187, for a view that consent alone never will protect children’s privacy adequately in an online environment..

extent of information control ceded to these companies.¹⁰⁵ On top of this, many children simply lie about their age in order to by-pass online consent mechanisms.¹⁰⁶

Recall that these privacy policies generally give to the company involved the right to sell what these companies consider “non-identifiable” personal information (such as websites visited, click stream path and any demographic information collected by registration on these websites – see discussion below) to third parties to assist in targeted marketing. Therefore children and parents don’t know, don’t care,¹⁰⁷ or never see what they are missing.

Second, Professor Steeves questions if consent, even “legally” obtained by the website/marketer, the present consent mechanism fails to account for children’s actual use of the Internet in relation to their developmental needs. Identity development is not what the purveyors of children’s websites, nor third party marketers, are seeking at any level. What they are seeking is profiling for better advertisement delivery and profit from sales of advertising.

The third point Steeves makes is that the constant collection of personal information from children (even if nominally consented to by the child/parent and even if tolerated as a necessary evil to help pay for the “online playgrounds” on the Internet), embeds a culture of, and creates a normalization of, surveillance of young people, from the time they are old enough to type (or have someone older type for them).¹⁰⁸

PIPEDA does, however, limit the usages of “personal information” that website operators and third party advertisers can make. “Personal information” under s. 2(1) of PIPEDA “means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.” This definition has been effectively widened or adapted to the Internet age by several findings of the Privacy Commissioner of Canada, who has declared in these findings, that IP Address, computer BIOS information, personal e-mail addresses and other information, are all “personal information” for the purposes of the Act.

¹⁰⁵ See the extensive report and conclusions by Jacquelyn Burkell, Valerie Steeves and Anca Micheti, “Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand” (March 2007), online: http://www.idtrail.org/files/broken_doors_final_report.pdf

¹⁰⁶ See above discussion of focus group interactions with privacy policies and “Broken Doors” report.

¹⁰⁷ See Valerie Steeves, “Lessons from Facebook’s Beacon”, *supra*, at p. 4 for the view that children do, however, care deeply about the concept and sense of privacy, though not about privacy policies *per se*.

¹⁰⁸ See V. Steeves, “It’s Not Child’s Play: The Online Invasion of Children’s Privacy” (2006), 3:1 UOLTJ, 169-188 (hereafter “Not Child’s Play”), at p. 172:

I argue that privacy laws have been ineffective for three reasons. First, the consent-based mechanisms they rely upon are easy to circumvent online. Second, current laws are limited because they fail to take young people’s experiences and social needs into account. And third, by focusing on procedural rules, privacy laws have constrained the potential for a broader debate on the social value of embedding surveillance into children’s private spaces.

What is notable about the definition of personal information under PIPEDA is not only that it is nearly all-inclusive but more importantly, it is defined as any information that is “about” an otherwise identifiable individual. If the information is about that person, it is “personal information” if it can, somehow, be associated with that individual, whether now or in the future, and whether or not the information is culled from many sources and compiled.¹⁰⁹

It is at this point that Canadian law diverges sharply from U.S. standards (which are largely fair information practices that are industry standard and are not legislated) and therefore from the practices of websites based in the U.S. In the U.S. the concept of “personally identifiable information” (PII) is used as a standard of privacy protection. In essence, any information that might identify or help to identify a person “in the real world” (or “offline” world), is covered by personally identifiable information. This generally means full name (not simply first initial and surname, for example) along with birthdate, home address or any number of government or business issued identifiers such as social security number, driver’s license number or credit card number. COPPA, the U.S. legislation regarding children’s privacy online, defines “personal information” for the purposes of the Act in a similar manner.¹¹⁰ In short, the U.S. term “personally identifiable information” or “personal information” under COPPA asks the question can a person be contacted, either in person or online, from the information.

In Canada, by contrast, PIPEDA requires consent to all collection, use or disclosure of personal information – which is simply some information about a

¹⁰⁹ Note that the European ARTICLE 29 DATA PROTECTION WORKING PARTY in WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June, online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf precises that if a party gains the “Means to Identify” someone, the information involved is personal information under EU law. It can include IP addresses and any other information gathered from the individual’s computer, voluntary provision of information or otherwise: “If, taking into account “all the means likely reasonably to be used by the controller or any other person” the information can possibly (as long as the possibility is not “negligible”) be linked to an individual it is personal information. Examples of such combinations of data to identify an individual are given in this document.

¹¹⁰ See subsection 8 of section 6501, which reads:

(8) Personal information

The term “personal information” means individually identifiable information about an individual collected online, including—

- (A) a first and last name;
- (B) a home or other physical address including street name and name of a city or town;
- (C) an e-mail address;
- (D) a telephone number;
- (E) a Social Security number;
- (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
- (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

person. Nothing in the Act, nor definitions, requires that the personal information be capable of uniquely identifying a person to the point of contacting them.

The result of this divergence is that U.S. website privacy policies regularly state what they will not do with PII, but do not address, or assume it is possible to deal in any way with, personal information (like IP address) as it is defined in Canada. The result is, these websites handle “personal information” about Canadian children but assume that their privacy policies have actually obtained consent to this use. In fact, based on Canadian law, for these elements of “personal information” that do not overlap with PII, they have not.

Neopets is a good example. The privacy policy is written to apply to both the U.S. and Canada (at one point there are references to “state/province” and “zip/postal code”).¹¹¹ Firstly, the site confusingly defines PII, as excluding “additional information that is not personally identifiable, such as city or state of residence or a visitor’s favourite cartoon character.” Such information, based on the definition of personal information in PIPEDA and OPCC findings, manifestly would be “personal information” under PIPEDA and therefore subject to PIPEDA’s consent and disclosure requirements. Neopets further makes distinctions without a difference by identifying “computer information” as another type of personal information it may handle outside the strictures of privacy law:

“Additionally, when visitors come to our site, we automatically collect some non-personally identifiable “computer” information, such as the type of computer operating system (e.g., Windows 95 or Mac OS), the user’s “IP Address”, the web browser (e.g., Netscape, Internet Explorer) being used, and information regarding the Internet service provider.”

As noted above, all of the “computer information” noted above has been considered by the OPCC in the past to be personal information for the purposes of PIPEDA and it all meets the threshold of the definition as “information about an identifiable individual” even if it does not, in and of itself, immediately identify that individual, only if there is that potential.

This makes Neopets statement that it protects personally *identifiable* information from disclosure to third parties without consent or parental consent ring hollow for Canadian personal information:

We will not use or transfer personally identifiable information in ways that are materially different from the ones described above without also providing parental notification of such practices and obtaining consent for any materially different uses.

This definition means that Neopets may transfer what they call “computer” or “non-personally identifiable” information to marketers without consent.

¹¹¹ See Appendix 1 for the text of the Neopets Privacy Policy.

Yet, were the more expansive definition of “personal information” under PIPEDA applied, and a more detailed and nuanced treatment of children’s capacity to consent also added to PIPEDA, it appears that much of the business models of immersive advertising and even third party targeted marketing would be greatly controlled. It is with this idea that we now examine other aspects of PIPEDA that can at present be called upon to limit the collection of children’s personal information online.

Principle 4.3.3 – “Necessary for the Purpose”

PIPEDA also limits what an organization may require by way of personal information in order to allow a person to use their product or service. Principle 4.3.3 limits the personal information that may be required as a condition of service, even if consent is given, to “that required to fulfil the explicitly specified, and legitimate purposes”. Extra information (beyond that required to provide the service) is not prohibited from being gathered, however, the organization may not require the person to give it prior to using the service or product.

This principle would seem to have great potential to change the present children’s websites that rely upon the immersive advertising business model. This is because, firstly, these websites invariably describe themselves as, and in practice operate as, online playgrounds. Nowhere in the privacy policy or terms of service is the business purpose – market research and targeted marketing – explicitly revealed to children or their parents. For example, Neopets describes what probably is individual clickstream tracking in this fashion in its privacy policy:

We sometimes use the non-personally identifiable information that we collect to improve the design and content of our site, to personalize our visitors' experience on Neopets.com, and to offer products, programs, and services. We also may use this information in the aggregate to analyze site usage, as well as to offer products, programs, or services.

It is unlikely a child, or even most adults would realize that “to personalize our visitors' experience on Neopets.com, and to offer products, programs, and services” is profile building and enables targeted marketing. It is certainly not specified “explicitly”. It is more difficult to imagine, however, how such collection and uses of personal information are required to present the simple gameplay available on this site to young children.

Therefore, any personal information collected beyond that necessary to play the games on the site or use basic communications features on the site, appears to violate this principle.

In addition, however, there is another requirement to principle 4.3.3. The explicitly specified purposes also must be “legitimate”. Legitimacy in this circumstance is not defined by PIPEDA. The concept has led to commentary that Principle 4.3.3 is difficult for both consumers and business.¹¹² In short, it is not clear whether the legitimacy is to be seen in the eye of the organization or the individual.¹¹³ However, it is certainly possible to conclude that the profiling and targeted marketing-enabling information collection is too surveillance-like to be “legitimate”,¹¹⁴ especially when the subjects of the data collection are young children.¹¹⁵

Reasonableness under s. 5(3)

Finally, PIPEDA has a general “reasonableness” requirement found in subsection 5(3) of the Act. This subsection qualifies the requirement to follow the dictates regarding consent and other matters in Schedule 1 by limiting the collection, use and disclosure to what a reasonable person would consider appropriate, in the circumstances (a classic legal subjective/objective test):

5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [Emphasis added.]

The Court in the *Englander* case, detailed above, viewed this section as an overall check on the reasonableness of any given information collection, use or disclosure.¹¹⁶ The provision of clickstream and other data tracking information used by children’s websites or those used by children in large numbers therefore should be required to pass this test of reasonableness.

The content of “reasonableness” has been described in cases considering subs. 5(3) as “protean” and depending upon the total factual situation in which it is applied.¹¹⁷ The case of *Turner v. Telus* in the Federal Court of Canada dealt with “voice prints” (basically recordings of voice characteristics) that the company

¹¹² See M. Long and S. Morin, *The Canadian Privacy Law Handbook*, 1st ed., (Canada: Centrum Information and Conferencing Inc., 2000) at p. 173. (“Privacy Law Handbook”).

¹¹³ See J. Lawford, “PIPEDA: How are we doing?”, at pp. 15-17.

¹¹⁴ See Privacy Law Handbook, *supra*, at 173: “Under clause 4.3.3, an individual could likely challenge marketing purposes as being non-essential. If an individual does not want their personal information used for subsequent marketing purposes, organizations should respect their wishes.”

¹¹⁵ See Steeves, *Not Child’s Play*, *supra*, at 187: “Once the broad-ranging impact of invasive marketing techniques on the development of a child’s identity and social relationships is brought into the privacy debate, it becomes much easier to conclude that that form of surveillance is not socially appropriate.”

¹¹⁶ See “PIPEDA: How are we doing?”, *supra*, at footnote 32 (pages 16-17) in that text.

¹¹⁷ *Turner v. Telus Communications Inc.*, [2005] F.C.J. No. 1981, at para. 41: “Privacy is a variable or changing concept, which is to say, a “protean” concept. Privacy rights are neither absolute at one extreme nor insignificant at the other. Their location on the spectrum between those two extremes is variable, depending upon the totality of the factual situation in which they are being examined.”

planned to use for verification of employees on its internal communications system.¹¹⁸ Some employees objected to the collection and use of their voice patterns. The Court held that Telus was acting reasonably in its collection and use, for a legitimate business purpose and that a reasonable person would consider it appropriate in the circumstances. The Court cited Supreme Court of Canada privacy decisions in search and seizure cases for the proposition that one must consider actual, real privacy risks in the collection and use and not merely speculative concerns about future uses and disclosures or data spills. The same Supreme Court cases also were cited for the proposition that if the information sought to be collected was generally being provided in public, that this mitigated against a finding that a collection or use was unreasonable. In the Telus case, the Court noted that the employees spoke to each other in the workplace in the usual course of employment and thus their unique voice characteristics were generally well-known to their employers and fellow employees.¹¹⁹

However, in the case of children's personal information such as clickstream data obtained on a "closed" children's playsite such as Neopets or Webkinz or Club Penguin, none of that information is regularly projected by the child to anyone else, only that website. Indeed, the business models of these sites rely upon the exclusivity of their access to this information.¹²⁰ In addition, the use of such information to deliver targeted ads or to tailor the website environment to the child is presently in use and is not an idle marketing fantasy of the future. Based on this view, it is certainly possible a court could determine that collection and use of children's personal information within a playsite like Neopets is unreasonable.

However, the narrowness of the legal approach to privacy taken from search and seizure cases also does not capture the public element of the debate adequately. Surely, given the concerns of social scientists and other academics with these sites as detailed above, parents and children should be concerned with the

¹¹⁸ *Ibid.*

¹¹⁹ *Turner v/ Telus, supra*, at para. 42.

¹²⁰ See Neopets FAQs, <http://info.neopets.com/presskit/faqs.html>, which, according to the Internet Archive "Wayback Machine" was online until November of 2007, but now is removed, states in part:

What is the business model for Neopets and how does the company generate revenue?

[. . .]

Online market research has played an important role in site content development, product development, concept testing and public relations from the Company's inception. In addition, market research has also become a source of revenue. Neopets' unparalleled access to young people, coupled with the Company's highly sophisticated, proprietary market research system, enables Neopets to conduct detailed consumer studies for companies that target young people, including the hard to reach 12 and younger age group. Neopets has the largest COPPA compliant (Children's Online Privacy Protection Act) online market research panel in the world, containing more than 50,000 12 and younger panelists complete with written parental permission. Neopets research is used by numerous Fortune 1000 companies, and is frequently quoted in respected publications such as Advertising Age and Television Week.

reasonableness of building immersive environments that mimic playgrounds only to extract market research information. On this basis alone, the Neopets model playsites are on this view not collecting and using childrens information “for purposes that a reasonable person would consider are appropriate in the circumstances.”

FOREIGN LEGISLATION

A study of legislation outside Canada shows that many major countries realize the need to curb at least some marketing practices in order to maintain and protect the privacy of children when they are online. However, the protections offered by other countries, while making some accommodation of children’s privacy, generally proceed only on fairly crude bases of age alone or parental consent. One law, however, has profoundly shaped the online privacy experience of children in Canada, the U.S. and around the world: the *Children’s Online Privacy Protection Act* (COPPA). It is to this law and its effect that we now turn.

The United States’ Children’s Online Privacy Protection Act

The *Children’s Online Privacy Protection Act* (COPPA)¹²¹ came into effect on April 21, 2000 and applies to the online collection of personal information from children under the age of 13. The rules within it spell out what a website operator must include in a privacy policy, when and in what manner they must seek verifiable consent from a parent and what responsibilities an operator has to protect children’s privacy and safety online.

Anyone who operates either a commercial website or an online service directed to children under the age of 13 that collects personal information from children or operates a general audience website and has actual knowledge that they are collecting personal information from children, must comply with the *COPPA*.

In determining whether a website is “directed to children,” the Federal Trade Commission (FTC) considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the website is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.¹²²

¹²¹ 15 U.S.C. 91, §§ 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728. See also the FTC’s COPPA Regulation, 64 Fed. Reg. 212.

¹²² <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.shtm>

To determine whether an entity is an “operator” with respect to information collected at a site, the FTC will consider who owns and controls the information; who pays for the collection and maintenance of the information; what the pre-existing contractual relationships are in connection with the information; and what role the Web site plays in collecting or maintaining the information.¹²³

The *COPPA* and its main safe-guard to the collection of children’s private information, rule 6502(b)(1), apply to individually identifiable information about a child that is composed online, such as **full name**, home address, email address, telephone number or any other information that would permit someone to identify or contact the child including, hobbies, interests and information collected through cookies or other tracking tools tied to individually identifiable information.

Rule 6502(b)(1) implements the requirements of the *COPPA* by requiring operators of websites or online services directed to children and operators of websites or online services who have actual knowledge that the person from whom they seek information is a child to:

1. Post prominent links on their websites to a notice of how they collect, use, and/or disclose personal information from children;
2. With certain exceptions, to notify parents that they wish to collect information from their children and obtain parental consent prior to collecting, using, and/or disclosing such information;
3. Not to condition a child's participation in online activities on the provision of more personal information than is reasonably necessary to participate in the activity;
4. To allow parents the opportunity to review and/or have their children's information deleted from the operator's database and to prohibit further collection from the child; and
5. To establish procedures to protect the confidentiality, security, and integrity of personal information they collect from children.

As directed by the *COPPA*, the Rule also provides a safe harbour for operators following Commission-approved self-regulatory guidelines.

One of the perceived benefits of the *COPPA* regime is the ease of compliance and the peace of mind it provides users when online. In order to fully comply with the *COPPA*, Section 312.4(b)(1) requires that an operator post a link to a notice of its privacy and information practices on its website homepage or online service and in any area of its site where personal information is collected from children. This link in itself must be clear and prominent and distinguishable from other links and areas of the website.

Section 312.4 (b)(2) of the *COPPA* clearly sets out the requisite content of the notice and details the information that operators must include in their notice on

¹²³ <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.shtm>

the site. This information is also to be included in any notice to parents under Section 312.4(c)(1)(i)(B) operators are specifically required to include in their notices:

1. Names and contact information for all operators;
2. The types of personal information collected through the site and how such information is collected;
3. How the personal information would be used;
4. Whether the personal information would be disclosed to third parties, the types of businesses in which those third parties are engaged, whether the third parties have agreed to take steps to protect the information, and a statement that parents have the right to refuse to consent to the disclosure of their child's personal information to third parties;
5. That the operator may not condition a child's participation in an activity on the provision of more personal information than is necessary to participate in the activity; and
6. That the parent may review, make changes to, or have the child's personal information deleted.

The *COPPA* regime also creates extra safeguards when operators want to disclose a child's (that is, a child under 13) personal information to third parties or make it publicly available. In order to do so, operators are required to utilise a more stringent and reliable form of consent. The methods to obtain this extra consent are outlined in the *COPPA* and include obtaining a signed form from the parent via regular mail or facsimile, accepting and verifying a credit card number in connection with a transaction; taking calls from parents through a toll-free telephone number staffed by trained personnel, or an email accompanied by digital signature.

Criticisms of COPPA Approach

However, the *COPPA* regime has created perverse effects. First, the low age threshold of 13 years old appears inadequate to capture even the "mature minor" category in law and most other advertising practice. Our focus group members aged 11-13 displayed notably less understanding of data sharing practices and privacy policies in general than our focus group members aged 14-17. Second, children routinely circumvent the self-reporting age reporting steps in registration on websites, knowing full well that there is no effective age verification system and that the "best" portions of these websites are available to users over 13. Third, by making children under 13's information effectively unavailable to third parties (due to the difficulties in obtaining explicit consent), *COPPA* has effectively encouraged the "Neopets model" that is, the immersive advertising experience for young children and has encouraged Neopets and others to extensively profile their guests internally, in order to be able to market this "demographic". Lastly, *COPPA*'s narrow prohibition only on the use of "personal

information” that is “individually identifiable information”¹²⁴ excludes huge amounts of what is considered “personal information” under many other countries’ personal information protection laws, including Canada’s.

According to the Federal Trade Commission (FTC), problematic activities that continue under the COPPA regime are “marketing back to a child based on his or her preferences or communicating promotional updates about site content.”¹²⁵ Although the FTC notes that such internal uses are only allowed once the operator has taken additional steps to increase the likelihood that the parent has, in fact, provided the consent, this verifiable parental consent can be difficult to obtain in reality. In any case, the FTC’s comments cover only children 12 and under, not those 13 and above.

Furthermore, as Steeves has pointed out, the fact that parents must give their explicit consent in the *COPPA* regime is not in itself a failsafe scheme to protect privacy of the youngest (under 13s). This is due to the fact that it is not only children who do not understand privacy policies, but often their parents as well.¹²⁶

Finally, the Electronic Privacy Information Centre (EPIC), on its “COPPA Page” notes the criticisms of COPPA being essentially an age verification system – and age verification systems generally don’t work, especially in the circumstances of children, who have an incentive to misstate their age to participate in activities supposedly reserved to older children, and have unintended constitutional and economic drawbacks.¹²⁷

¹²⁴ See subsection 8 of section 6501, which reads:

(8) Personal information

The term “personal information” means individually identifiable information about an individual collected online, including—

- (A) a first and last name;
- (B) a home or other physical address including street name and name of a city or town;
- (C) an e-mail address;
- (D) a telephone number;
- (E) a Social Security number;
- (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
- (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

¹²⁵ <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.shtm>

¹²⁶ Broken Doors, p. ?, fair game? P. ?

¹²⁷ See Electronic Privacy Information Center, “The Children’s Online Privacy Protection Act (COPPA)”, online: <http://epic.org/privacy/kids/> at heading “Criticism of COPPA: Constitutional and Economic Drawbacks of the Verification Systems”:

“Critics have claimed that the methods outlined by the FTC for verification - sending/faxing signed printed forms, supplement of credit card numbers, calling toll-free numbers, or forwarding digital signatures through email - are too costly, cumbersome, and inadequate in protecting personal information. Even though new technologies are being developed, the current verification methods are too slow and impractical. The process of verification of mails, emails, and credit card

The UK's Dual Approach Part I - The Privacy and Electronic Communications (EC Directive) Regulations

The *Privacy and Electronic Communications (EC Directive) Regulations [Regulations]* came into force in the UK on December 11th 2003. Unfortunately, the *Regulations* do not distinguish between adults and children, giving both the same rights and resultantly treating both the same. Nevertheless, the regime calls for consent from all individuals prior to the collection and disclosure of their data under s. 7. As a result, online and mobile services providers must ensure that children have been provided with the opportunity to decide whether to give their consent or not.

Yet, the *Regulations* leave the door open for websites to utilize the information collected from children once nominal consent is given. Section 7 details that the data relating to an individual may be processed and stored by a provider of a public electronic communications service if it is for marketing electronic communications services, or for the provision of value added services to that user; and consent has been provided.

The UK's Dual Approach Part II - The *Data Protection Act*

The United Kingdom's *Data Protection Act (Act)* was revised from an earlier 1984 edition and brought into effect on March 1, 2000. The *Act* expands the breadth of the 1984 edition by distinguishing personal data and sensitive personal data. The latter includes racial or ethnic origin, political opinions, religious beliefs, data regarding sexual preferences and lifestyles, and physical or mental health. Children's data is not listed as per se sensitive.

Under Schedule 2 of the *Act*, in order to process all personal data a website must ensure that the data subject has either:

numbers may take over a day. Further, disclosure of credit card information will expose the parents to the same privacy risks that they are trying to protect their children from and deter them from using such online services in general. As a consequence, children may manipulate information to access these websites, and in the long run, online businesses may either eliminate children-focused sites. Some sites simply claim that they do not sell products to children, and therefore do not need to comply with COPPA. An example for such a site is Amazon.com, where the online privacy notice states that no products are sold to children, and such products can be purchased only by people over 18 or with the involvement of a parent or guardian.

Even if websites do develop technology that enables easier compliance with the verification requirement, an important constitutional issue will remain unsolved. As EPIC has testified, any personal identification requirements from Internet users as a condition to access online content chills free speech and infringe on the First Amendment right to communicate anonymously.”

1. Given consent or;
2. The processing is necessary:
 - a) For the performance of a contract to which the data subject is a party;
 - b) For the taking of steps at the request of the data subject with a view to entering into a contract;
 - c) To comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
 - d) In order to protect the vital interests of the data subject.
 - e) For the administration of justice;
 - f) For the exercise of any functions conferred by or under any enactment;
 - g) For the exercise of any functions of the Crown, a Minister of the Crown or a government department;
 - h) For the exercise of any other functions of a public nature exercised in the public interest.
 - i) For the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

In terms of sensitive personal data; one of the above conditions for all personal data must be satisfied and:

1. The data subject must give explicit consent to the processing of the personal data, or;
2. The processing of the data must be necessary:
 - a) For the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment
 - b) In order to protect the vital interests of the data subject or another person, in a case where
 - i. Consent cannot be given by or on behalf of the data subject, or
 - ii. The data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - iii. In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld, or;

3. The processing:

- a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit;
- b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and
- d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

The *Act* also contains eight “Data Protection Principles” (Principles), which serve as the foundation of the UK’s legislative privacy scheme and are occasionally referred to as the “Principles of good information handling”. The Principles, set out in Part I of Schedule 1 of the *Act*, apply to all personal data processed by data controllers unless a data controller is able to claim an exemption from any of the Principles under Schedule 4 of the *Act* (national security, crime and taxation, health, education etc.). However, data controllers must notify the Information Commissioner whenever they collect personal data.

These eight Principles are as follows:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the *Act*.
7. Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Under the *Act*, these Principles compel website operators who collect personal information from individuals to adhere to specific practices. In short websites must:

1. Ensure web collection forms comply with “fair processing” principles i.e.: identify the organization to users; explain why the site is collecting the data, and the third parties they will pass the data to (both internally and externally).
2. Ensure the security of the data collection process and inform users when the website intends to use cookies or web bugs (beacons) and provide the opportunity to refuse the cookie.
3. Post a privacy policy and provide links to it at every point of information collection.
4. Provide an "opt-out" mechanism for receiving direct marketing email.
5. Ensure a valid email address is used for direct marketing purposes.
6. Ensure that when information is collected from children under 12, they understand how their information is being collected and used. Parental consent must be obtained for those under the age of 12, and there must be a way to verify that the consent has been given.¹²⁸

In their combined capacity, the UK’s dual legislative approach appears to create a strict regime when it comes to general online privacy.

However, given the lack of specific rules relating to children or minors, it is open to the U.K. based website to accept “consent” from any child. The U.K. Data Commissioner has issued “Guidance” on the issue of consent from minors, however, that indicates that a child of 12 is capable,¹²⁹ if he or she understands, in general, the nature and consequences of consenting to data collection, use and disclosure, in parallel with U.S. COPPA (but one year earlier).

In this environment, websites and online services in the U.K., much like in the United States and Canada, are permitted to receive consent directly from children aged 12 or 13 and up.

The Way Forward: Legal and Policy Recommendations

In the result, there appears to be a vacuum in terms of legal controls of personal information use of children and teenagers in online electronic commerce that risks serious privacy violations. It is doubtful that present advertising industry standards are sufficient to protect children in the new business models of

¹²⁸ <http://www.watchfire.com/securityzone/dpa.aspx>

¹²⁹ See also U.K. *Data Protection Act, 1998*, s. 66. Source: Information Commissioner (U.K.), Data Protection Act 1998: Legal Guidance, online: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

immersive advertising and social networking. In any case, voluntary codes are only applicable to industry members of such organizations and have a track record of not being enforced despite ostensible audit provisions.¹³⁰

It is an open question if PIPEDA, properly understood and enforced, could apply appropriate legal standards. CIPPIC effectively has argued that PIPEDA provides the tools to curb abuses in the social networking sphere. CIPPIC's analysis does not appear to fully cover immersive advertising websites such as Neopets, however. In such cases, perhaps the concept of informed consent, with appropriate scope for a mature minor rule and a robust interpretation of subsection 5(3) (reasonableness) of PIPEDA could provide adequate protection for children and teens regarding their personal information in Canada.

However, we think not, and rather that more prescriptive changes to PIPEDA are required, along with adequate enforcement mechanisms.

Clarifying Children's Consent under PIPEDA

As stated in the *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics* (Fourth Report),¹³¹ the Canadian Bar Association (CBA) has argued that under *PIPEDA* "there is uncertainty about whether minors can consent to participate in on-line activities without parental consent."¹³² As a result, the CBA called for clarity on whether minors can give consent and implementing a regime where children below a certain age cannot consent without first obtaining the approval of their parents or legal guardians.

One need go no further than the Fourth Report to see that the idea of a consent mechanism within *PIPEDA* is a heated point of dispute. The Committee itself was

¹³⁰ See Harris Testimony, supra, at p. 17 and Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf at 16-17.

¹³¹ Standing Committee on Access to Information, Privacy and Ethics, House of Commons, "STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA), Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics" (Ottawa: House of Commons, May 2007) (Fourth Report). Online: <http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/ethirp04-e.pdf>. See also the Minister of Industry, "Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics" (July 2007) (Government PIPEDA Response). Online: [http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/\\$file/ETHI-e.pdf](http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf). Note that the Minister in this Report stated:

The government recognizes that the privacy of minors can be vulnerable, particularly in an online environment. In support of the Committee's recommendation, the government will consult with relevant stakeholders to examine the issue of consent by minors, and to consider the necessity and feasibility of amending PIPEDA in this respect.

¹³² Fourth report p. 28

formed in 2007 to undertake a statutory review of *PIPEDA* with recommendations to any necessary amendments. In the end, the Committee, heard from various sources regarding privacy in general, and the personal information of minors in particular.

Throughout all the recommendations, the common theme of a stronger consent mechanism being a necessity in *PIPEDA* was prevalent. Valerie Steeves pointed out that the present legislative scheme in Canada permits companies to set up online environments that utilise the weak consent mechanism of *PIPEDA* to capture the private information of children and reconfigure it as a commercial commodity.¹³³

Philippa Lawson, of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), also brought to light the inadequacy of *PIPEDA* with regard to the collection, use and disclosure of children's private information, as well as strict penalties for violating any such provisions. PIAC made similar submissions.¹³⁴

PIAC at that time doubted that consent alone, of either parent or child, could be made meaningful in light of the structure of children's websites. PIAC thus recommended an alternate approach of banning targeted secondary marketing to children as part of a new subsection under *PIPEDA*'s reasonableness clause (5(3)). However, with the present report, PIAC considers that a more structured approach to consent under *PIPEDA* for children's personal information may go further in protecting children's privacy than an outright marketing ban, while still permitting legitimate websites and services to be offered to children.

The House of Commons Committee itself noted the thorny issue of establishing a specific age at which children are found competent to act independently, since that generally is a matter of provincial jurisdiction and the courts. Even so, the Committee saw fit to suggest that the issue of consent with respect to the collection, use and disclosure of personal information from minors in a commercial context was of sufficient importance to merit further study with a view to amendments to *PIPEDA* in this regard.¹³⁵ We support the idea of further study of this issue but are concerned with that the delay in awaiting further research results may endanger children as significant personal information is continued to be used in a commercial context in the meantime.

We submit therefore that clear consent rules should be enacted in *PIPEDA* now, and that the jurisdiction to set specific consent rules flows from the federal

¹³³ Fourth report at p. 27

¹³⁴ PIAC followed up this appearance with a written submission to Industry Canada with regard to the Government *PIPEDA* Response (see footnote above) on reform of children's privacy under *PIPEDA*. See PIAC, "Submission to Industry Canada Considering the House of Commons Standing Committee on Access to Information, Privacy and Ethics' Report on the 2006 Review of the Personal Information Protection and Electronic Documents Act (*PIPEDA*)" (Ottawa: PIAC, 2008) at pp. 7-9 . Online: http://www.piac.ca/files/piac_submission_to_ic.pdf

¹³⁵ Fourth Report p. 28-29

government's jurisdiction over privacy under its trade and commerce power, the power cited to pass PIPEDA. In short, the federal government, in amending PIPEDA to provide for different consent rules in relation to various ages is not regulating legal ages of majority for provincial purposes but setting rules for consent in the context of privacy law in PIPEDA. Such rules can vary based on age as demonstrated by research and policy that various ages of children perceive privacy differently, and have varying capacities to understand consent and privacy policies.

Industry Canada, speaking on behalf of the Canadian Federal Government, recognized that the recommendation by the Committee to examine the issue of consent by minors with a view to amendments was a just one as the privacy of minors can be vulnerable, particularly in an online environment.¹³⁶ We support this emphasis on children as a vulnerable population that deserves special rules regarding privacy.

Recommendation 1: Amend PIPEDA to provide clear consent rules for children

This uncertainty over children's consent to the use of their personal information should be definitively regulated by amending PIPEDA to provide clear consent rules for various ages of children, as is done in the CMA Code of Conduct.

Based on the research detailed in this report and the indications of focus groups, PIAC therefore recommends the following clear consent rules for children and teens under the age of majority in any province (18 or 19 depending upon province):

Summary of Proposed PIPEDA Consent Provisions

Age	Type of Information	Consent Requirement
Under 13	Any personal information	Collection, Use or Disclosure Prohibited
13, 14 and 15	Any personal information	Collection and Use: only for collecting site.* Opt-in consent is by teenager <u>and verifiable, explicit consent required of parent or guardian.</u> Disclosure prohibited.

¹³⁶ Government PIPEDA Response at p. 8.

16 and over	Any personal information	Collection and use: only for collecting site*; opt-in consent by teenager Disclosure: Opt-in consent is by teenager <u>and verifiable, explicit consent required of parent or guardian.</u> Upon Majority: Explicit consent of new adult to continued retention and future use or disclosure of data collected while a child
-------------	--------------------------	--

*Note: A collecting site may be a social network, in which case, “use” would include posting (disclosure) of profiles for use of other members within that social network, provided clear notice of this use were provided to the teen and parent at registration.

Children Under 13

PIPEDA should be amended to prohibit the collection, use or disclosure of personal information of all children under 13 years of age. This proposal is stricter than that of COPPA in the United States, which allows such collection and uses if a parent’s verifiable, explicit consent is obtained. Given the extreme vulnerability of this age group and lack of comprehension of privacy rights, the demonstrated market desire for this information and the dangers of such systems upon child development identified by researchers, it is the only safe course to make the personal information of children wholly private. Such a requirement would bring Canada largely into line with other countries that have effectively decreed this age group as sacrosanct and not to be profiled.

Younger Teens (13-15)

Regarding teenagers who are 13-15 years of age, while there appears to be some maturation in terms of understanding privacy, teenagers’ concepts of privacy diverge too sharply from that of adults to make any expression of consent to market uses of their personal information reliable. We considered that a safer course would be to make this age group legally incompetent to consent to their private information being collected, used or disclosed online, like younger children, but to allow parents to consent via an explicit consent mechanism. Capacity to consent is limited at this age. However, this requirement would effectively require the dismantling of many popular websites for children.

Nonetheless, the concepts of target marketing, immersive advertising and the full implications of exposure on social networking seem largely lost on this age group. However parents, in consultation with their child, may be better placed to weigh the potential gains from entering commercial playsites than government – provided there is a meaningful description of the true nature of the collection and use of personal information required to run these websites and services.

As a result, we would recommend seeking opt-in consent of the teenager and, in addition, explicit, verifiable consent of an adult to any use or collection of personal information from children of this age group that a website claims is necessary to run the website. It is hoped that the requirement of explicit consent of a parent would encourage a discussion between parent and child about the use of personal information by the site and the potential trade-off of privacy for the service.

However, as a key extra safeguard, any disclosure to any third party (including the main website's corporate affiliates) would simply be prohibited. In this way, those websites that rely upon the collection and use of personal information to product place and to deliver targeted advertising to this age group could only operate provided the product placement and targeted advertising were done on an aggregate level or, if targeted to a particular child, that only that website had that particular child's profile and could not share it. Such a restriction leaves websites operating on the immersive model able to continue operating while reducing their reliance on third party disclosure for revenue. In addition, if a website collects and uses personal information of this age group to finance itself in any way, the disclosure of this fact to the parent and child prior to their consents, in clear and simple language, should be required to ensure truly informed consent to this surveillance-type advertising model.

Finally, this change to PIPEDA would have to clarify that collection and use of personal information for a social networking site (for example, by creating a profile of children this age and letting their friends link to it), while technically a "disclosure" for the purposes of PIPEDA, should be permitted. We suggest that a simple manner to draft this would be to prohibit any "commercial" disclosure.

Older Teens (16 to majority)

Older teens appear to have a greater understanding of privacy matters and a generalized conception of websites that target them as a money-making venture, but appear to lack full appreciation and understanding of the extent to which their personal information drives the various child website models.

Recognizing the growing maturity of these teens and their expanding ability to weigh privacy trade-offs, while simultaneously encouraging caution in highly personal information-intensive services such as social networking, PIAC recommends that teens of this age should be permitted to consent to collection and use of their personal information inside a particular website or service (including within a social networking site – see above), but that that website not be permitted to disclose that personal information without the opt-in consent of the teen and the verifiable, explicit consent of a parent or guardian.

As such, popular social networking sites could indeed collect and “use” personal information within the confines of their sites for the stated purpose of their existence, namely social networking, but may not trade on such information to finance themselves without full disclosure of this purpose to not only the teen but a parent or guardian. If those consents were obtained, third party targeted marketing of these children, and the disclosure necessary to facilitate it, would be permitted (in accordance with the third party’s privacy policy). Again, this requirement to seek parental consent for third party disclosures should trigger discussions of appropriate personal information disclosure in any particular household. It also should wean these sites off of reliance upon third-party advertising financing to offer such a service, unless they are so upfront as to clearly describe this model and seek the informed participation of these teens and their parents. While parental consent may seem unnecessary at this level of child development, the consequences of third party profiling are too great, and appear to be too poorly understood by this age group, to risk the privacy involved without parental knowledge and consent. In our view, consenting to online marketing which relies upon personal information is not a situation exactly akin to a medical treatment, as it is not as “life and death” as consent to medical treatment, a different standard than “mature minority” may be appropriate.¹³⁷ We feel parental involvement for third party marketing disclosures is necessary and appropriate.

Finally, in order to protect children as they move to adulthood and fully comprehend the enormity of the potential information holdings gathered while they were still a minor, PIAC recommends that any website that has legitimately collected or used personal information while the child was a minor be prohibited from retaining it, using or disclosing it after a child’s majority by being required to seek explicit, opt-in consent to this continued retention, and further use or disclosure for any purpose during the child’s adulthood. In other words, on the child’s eighteenth birthday, the website would have 60 days to contact the former child to seek such explicit consent to continued retention, use, or disclosure of a former child’s personal information or be forced to destroy it within a predetermined time (taking into account the PIPEDA principles of Individual Access and Challenging Compliance), most likely one year.¹³⁸

This requirement will provide the child/adult with the ability to discard their childhood profile and move into the adult world without being typecast based on their childhood information holdings. This is a particularly valuable right in light of the extensive surveillance of childhood playsites. This requirement resembles young offender laws that seek to allow teens a fresh start upon reaching

¹³⁷ On this important point see the description of “Gillick competence” and its limits in an organized information collection and gathering system (child protection databases, which in some sense are akin to large commercial marketing databases) in Foundation for Information Policy Research, “Children’s Databases – Safety and Privacy: A Report for the Information Commissioner” (London?: FIPR, November 2006), Online: http://www.fipr.org/childrens_databases.pdf

¹³⁸ This would also allow adequate time for the former child to continue any social networking site profiles he or she had created without disruption.

adulthood by making their juvenile record largely unavailable in future proceedings. As much as such youth criminal justice subjects deserve this chance, it can be argued that equal regard should be given to those with a long “information record” whose only transgression was use of corporate websites targeting children. This requirement would also provide the companies involved with another opportunity to seek individual adult consent with regard to their services. Such a requirement would, for example, require social networking sites to delete personal profiles and all references to identifiable individuals within their services if they did not receive the required consent in the required time.

Recommendation 2: Visible, clear and understandable signs of collection, use and disclosure

Privacy policies are generally not read or understood by child and teen users. Thought should go into designing clear pictograms that quickly alert a potential child user to the level of information collection and sharing undertaken by a website. These icons could be developed by the Office of the Privacy Commissioner of Canada as part of that office’s focus on children’s privacy.

Such a proposal was made by Simson Garfinkle in relation to another confusing area for consumers, spyware. His proposal used the following icons to explain the main aspects of spyware.¹³⁹









 <p>Hook Hooks itself so that it runs at boot.</p>	 <p>Modify Modifies your computer’s operating system.</p>	 <p>Monitor Monitors what you are doing even when not the active application</p>	 <p>pop-up Displays pop-up windows, even when not active application.</p>
 <p>Self-updates Downloads code from the net that could change its behavior.⁴</p>	 <p>Dial Can dial a phone (and spend your money!)</p>	 <p>Sticky Cannot be uninstalled.</p>	 <p>Remove Application allows others to remote-control your computer</p>

Figure 1: A few icons that could be required by federal regulation.

Similar simple pictograms should be both interesting and informative for a younger audience schooled in a more visual communication and learning environment that the Internet provides.

Personal information symbols would include icons showing: whether the website collects personal information, what information is collected, the manner in which personal information is used by the website, and with whom who the website

¹³⁹ These icons are reproduced with the kind permission of Mr. Garfinkle in the PIAC report “Spyware: Looking Out for Consumers” (Ottawa: PIAC, 2005) at p. 66. Online: http://www.piac.ca/files/spyware_piac_report.pdf

shares this information. Icons for third party advertisers should be included and indicate that these third parties use the personal information for financial gain. Other icons could show retention times for personal information and whether information was shared with law enforcement. The symbols also should include references to the ages of participants if PIPEDA is amended to provide different consent and other requirements for various age groups.

These symbols would not replace the requirement to post a privacy policy, rather, they will help alert the child user to the general level of information required of the child to participate in the website before the child enters into the registration process, which children may be anxious to complete in order to play the game.¹⁴⁰

Recommendation 3: Draft privacy policies children can understand

As stated in their 2007 “Broken Doors” report; Burkell, Steeves and Micheti recommend utilizing the simplest words and providing clear definitions wherever possible, as the majority of children that participated in that study expressed difficulty with the language and legal nature of privacy policies.¹⁴¹ Some children believed websites purposely sought to capitalize on the complex language to undermine the children’s ability to understand what they were engaging in.¹⁴² Children’s websites concerned about their standing in the child and teen community therefore should be open to a more transparent statement of their privacy policies.

The Office of the Privacy Commissioner of Canada commissioned the “Broken Doors” report and it is hoped that the OPCC will be working on providing plain language and age appropriate drafting guidelines for businesses in the child website market as part of that office’s focus on children’s privacy.

¹⁴⁰ See Environics Report, p. 51, 52:

M: Well for example, have you ever read one of those contracts when you go on a site? You know the ones that I mean when it has word, word, word, word, word, word?

R: They’re usually like, the first time I was like, the first time I saw one of those, I started reading just the top, the first paragraph and I was just like okay, this is getting really boring, I know what to do on the site already. I know how it works; I know what goes around on the site so I just press, I accept the terms.
[. . .]

M: How about you? Have you ever read one?

R: When I first made my account on Roomscape [sic, RuneScape], they had a really, really long one. I read the first bit and then I just skipped through it and said yes.

¹⁴¹ Steeves, “Broken Doors”, *supra* at p. 23

¹⁴² Steeves, “Broken Doors “, *supra* at p. 24

The OPCC should also be empowered to make mandatory guidelines for required disclosures in privacy policies, along the lines of the *COPPA* regime, section 312.4(c)(1)(i)(B).

Recommendation 4: Specific regulations for social networking sites

Social networking sites such as Facebook and MySpace involve such extensive collection, use and display of children's personal information and are so attractive to children and teens due to their developmental needs that these "Pied Pipers of the Internet" require extra rules to safeguard children's personal information.

First, privacy settings for child users should be automatically set to the highest (most private) settings available by default. For example, Facebook's Beacon should be turned off by default for children and viewing children's profiles should be restricted to friends authorized by the child only, not automatically made available to all network members in the networks the child joins, nor to the whole Facebook user community. Second, profile searches (either within the community or the Internet at large) by age or similar category that consistently can produce results listing child profiles should be made illegal under PIPEDA. Third, children should have the option of using a pseudonym for their online profiles, not their real names.¹⁴³

Recommendation 5: Privacy Commissioner should enforce the new regime with new fining power; Audit powers

The Office of the Privacy Commissioner of Canada (OPCC) should be granted power to impose financial penalties to encourage enforcement of the new PIPEDA sections on children's privacy. These "administrative monetary penalties" (AMPs) should be flexible but potentially significant to encourage compliance. Recent amendments to the *Telecommunications Act* to enforce the National Do Not Call List give the Canadian Radio-television and

¹⁴³ This recommendation comes from the International Working Group on Data Protection in Telecommunications, "Report and Guidance on Privacy in Social Network Services – Rome Memorandum" (2008)" at p. 6. Online: http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf Footnote 23 of the Rome Memorandum notes that pseudonymous access to such sites is probably not absolute (that is, the site likely will have to know the child's identity). Under the rules proposed in this report, a website could keep such contact information for identity verification and indeed likely would have to do so in some way to ensure age verification. However, since this information could not be shared with third parties (except for those teens aged 16-majority and with parental consent) this knowledge of real name should not pose as many privacy issues as social networking sites that "require" a real name and contact information to use the service. This report also calls for the highest privacy settings for users by default.

Telecommunications Commission (CRTC) the power to impose AMPs of up to \$1500 per violation for an individual and up to \$15,000 per violation for a corporation. A similar scale of AMPs should be made available to the OPCC for violations of children's privacy under an amended PIPEDA.

Such fining powers are necessary in order to move responsibility for designing age verification systems that work more to be the responsibility of children's website providers, rather than the households that are signing up. Facing a fine for collecting underage children's personal information should

In addition, the OPCC should use its present audit powers to investigate the children's website market, including immersive advertising model sites and social network sites subscribing Canadian children to ensure compliance with the new bright line consent rules.

Recommendation 6: Government should Support or Create Non-commercial Online Playspaces

Governments should support the development of non-commercial public online playsites as an alternative to the commercially structured models that children now overwhelmingly use. Such sites should be designed to collect no personal information about children whatever.

At present, children have little real alternative to the commercial playground when they go online. Certainly there are few non-commercial sites, if any, offering anything like the attractive and interactive graphics and games on the commercial playsites. Having non-commercial websites should provide children and their parents with a choice regarding online play and should provide them with a chance to experience online play without surveillance.

In the alternative, the federal and provincial governments should support non-commercial children's websites financially as a stand-alone policy goal of promoting safer online experiences for Canadian youth. Some of this funding could also be tied to websites that promote other Canadian cultural goals.

Recommendation 9: Coordination and Promotion of Child Privacy Rules Worldwide

There should also be efforts to coordinate privacy rules across jurisdictions so that any Canadian standards are not easily avoided. The OPCC should take on child privacy as a leading issue, which it appears to be tentatively already doing, and become world-standard-bearer for children's privacy rights. The OPCC should raise the issue of children's online privacy rights at future conferences of privacy commissioners. Ideally, the OPCC should push for an international instrument like the Convention on the Rights of Children regarding children's

privacy and marketing to children online, which would require national and regional data protection authorities to set minimum child privacy standards in their legislation by a set date.

Recommendation 10: Online Privacy Education for Youth

Children and teens should be taught the fundamentals of online profiling, third party advertising and immersive advertising in courses on computer literacy and safety that already provide information on more “personalized” threats such as grooming and cyber-bullying. Children and teens should be taught their privacy rights under PIPEDA (as it stands now and as amended) so that they themselves can identify potential breaches of the rights. Coordinators of online safety and literacy programs should liaise with the OPCC on course content and the OPCC should assist with preparation of information sheets and online tools such as further YouTube videos on children’s privacy rights.

Conclusions

Canadian privacy law provides little guidance specifically for collection, use and disclosure of children’s personal information online. Existing U.S. rules effectively permit unlimited access to personal information of children aged 13-18. In this environment, new Internet business models have developed that are largely advertising-driven and rely heavily upon the collection, use and disclosure to third parties of detailed personal information on children. In particular, immersive advertising websites that children view only as online playgrounds have achieved nearly critical mass amongst younger children. Older children have been attracted to another business model, social networking, in even greater numbers, as they seek out self-actualization and friendship in the Internet. Yet these environments are structured largely as surveillance and market research firms and the children are the oft-oblivious subjects of this market research.

The long-term effect of constant market surveillance of children and large-scale data collection has not been studied but initial social science research regarding this phenomenon is spectacularly negative. The indications from the Environics focus groups in this study tend to support some of the conclusions of this initial research and also lead to interesting questions about children’s perception of market surveillance. Further research on the various online businesses that collect children’s personal information is therefore warranted.

However, what is more troubling is that the creation and growth of these websites is possible despite the present fairly extensive privacy law regime in Canada. It appears doubtful that the consent-based regime in Canada is up to the task of providing adequate protection for children’s personal information in Canada.

More specific rules are needed to address children's privacy online in Canada. Waiting for further research before making changes to privacy law to protect children may not be the wisest course. Parliament should act now, as part of its review of PIPEDA, to add the privacy rules suggested in this report or similar ones.

In the meanwhile, children, teens and parents should realize that by entering almost any online playsite, children are already members of a new family on the other side of the computer screen, the "data family".

Appendix 1 – Environics Research Group Report on Focus Groups

“All in the Data Family? Databases, Children and Profiling: A Qualitative Exploration” Environics Research Group (January 2008)

Appendix 2 – Neopets Privacy Policy

Neopets Privacy Policy

Neopets.com is committed to providing a fun, entertaining, and safe Web site for people of all ages. We are dedicated to safeguarding any personal information collected on-line and to helping parents and children learn how to exercise control over personal information while exploring the Internet. To this end, we ensure that our privacy policy and our information practices adhere to the U.S. Department of Commerce's Safe Harbor Principles. Because many of the visitors to this site are children, we take care that our content is suitable for children. In addition, we take special measures to help children protect their privacy while on-line. For example, we do not ask children to disclose more personal information than is necessary for them to participate in a particular activity, and we take efforts to prevent children from posting contact information.

To help ensure a rewarding on-line experience for our visitors - and for the parents of our visitors who are children - we provide you with this summary of our information practices.

As we continue to offer our visitors new and different types of content and services, we may modify our practices from time to time. However, we will treat all personal information we collect in accordance with the privacy notice in effect at the time the information is collected.

I. The Information We Collect

At Neopets.com, the only personally identifiable information we collect from users 12 years old and younger is a valid e-mail address. And, we ONLY use this information to send these users one message to activate their Neopets account, and then the e-mail address is completely removed from our system. We also ask users 12 years old and under for certain non-personally identifiable information, such as birth date, gender, state/province, zip/postal code, and country.

Neopets requires users 13 years and older to provide a first and last name, valid e-mail address, birth date, gender, and postal code. Although they have the option to voluntarily enter additional information (such as home address, state and country), it's not a requirement to activate their account. For some of our on-line activities-such as polls or surveys-we may ask users to provide additional information that is not personally identifiable, such as city or state of residence or a visitor's favourite cartoon character.

Users can also change their user information supplied upon registration (except for user name, original e-mail address and date of birth) on this page:

<http://www.neopets.com/userinfo.phtml> and following the direction on such page. When a child under 13 enters a contest, we will ask for a parent's e-mail address so that

we can notify the parent that we have received personal information from the child. We do not knowingly collect names and e-mail addresses from children under 13 without notifying the parent via e-mail and giving them the opportunity to remove their child's name from the list of entries. Winners of our contests or sweepstakes are notified by e-mail, and are required to send us by fax or regular mail a form containing their street address. Winners who are minors must have the form signed by a parent in order to receive their prizes.

Additionally, when visitors come to our site, we automatically collect some non-personally identifiable "computer" information, such as the type of computer operating system (e.g., Windows 95 or Mac OS), the user's "IP Address", the web browser (e.g., Netscape, Internet Explorer) being used, and information regarding the Internet service provider.

II. How We Use the Information

We use visitors' personal information for our internal purposes of enabling visitors to enter one of our on-line contests or sweepstakes, to subscribe to our online newsletter, or to inform users of upcoming events and special announcements. We use the e-mail addresses of parents to notify them when we have received information from their children and to give them the opportunity to have their child's name removed from our lists. We do not keep any personal information we obtain through a contest or sweepstakes after the particular event is completed. We use the names and e-mail addresses of subscribers to our e-mail newsletter only to send them the newsletter. Each newsletter contains instructions on how to be removed from the subscription list by sending us a return e-mail. We also use visitor's personal information to track usage and to ensure user are following the site's Terms and Conditions.

Sometimes we will use agents or contractors to help us provide services to our visitors, such as helping us conduct a sweepstakes and sending prizes to the winners. In these cases, we require the agent or contractor to keep the information confidential and to use it only for the specific services they are performing. In addition, please review the section on Collection of Information by Third-Party Sites and Sponsors for a description of the limited instance whereby personal information collected on the site may be supplied to third parties with the consent of the user.

We sometimes use the non-personally identifiable information that we collect to improve the design and content of our site, to personalize our visitors' experience on Neopets.com, and to offer products, programs, and services. We also may use this information in the aggregate to analyze site usage, as well as to offer products, programs, or services.

We will disclose information we maintain when required to do so by law, for example, in response to a court order or a subpoena. We also may disclose such information in response

to a law enforcement agency's or other public agency's (including schools or children services) request or if we feel that such disclosure may prevent the instigation of a crime.

We will not use or transfer personally identifiable information in ways that are materially different from the ones described above without also providing parental notification of such practices and obtaining consent for any materially different uses.

III. Collection of Information by Third-Party Sites and Sponsors

Our site contains links to other sites, including those of sponsors, advertisers and survey companies, whose information practices may be different from ours. Sometimes the other sites might conduct contests or sweepstakes that are promoted on Neopets.com. Visitors should consult the other sites' privacy notices, since those sites are not covered by our privacy policy and may follow procedures that are different from ours. Neopets never gives a user's e-mail address or other registration information to such third parties without permission, however, if you choose to "opt-in" (click on a box to receive a third party's information), to register with one of our sponsors, or not to "opt-out" (uncheck a checked box that will provide a sponsor with your information), that means you have allowed Neopets to give your registration information and other collecting information, including e-mail address, to that that third party.

Additionally, sometimes third parties use cookies, text files, or similar technologies (see "IV. Cookies" below) to collect user preferences for various purposes. The use of these technologies by such third parties is subject to their own privacy policies, not ours. Visitors who do not wish their activities to be subject to this data collection should consult the websites of these third parties for their procedures for opting out of cookie placement.

IV. Cookies

Neopets.com uses a software technology called "cookies." Cookies are small text files that we and certain third parties place in visitors' computer browsers to store their preferences. Cookies themselves do not contain any personally identifiable information. Although cookies could enable us to relate a visitor's use of this Web site to personal information that a visitor has provided, such as an e-mail address, we do not use them for this purpose. We do use "cookies" to determine how many visitors we have and how often they visit various sections of our site.

We employ P3P codes and so-called P3P privacy policies only as technical switches to enable our web site to function properly. Some Web browsers require those codes in order to trigger the function of certain cookies. However, our use of P3P is completely unrelated to any privacy or data policies that we may be bound to and the DSA token in our compact P3P

privacy policy means that the P3P codes and so-called P3P privacy policies we publish have no meaning and carry no obligations or liability. We disavow any significance to those codes and policies and reject all aspects of the P3P protocol.

V. Security

We have put in place appropriate physical, electronic, and managerial procedures to safeguard and help prevent unauthorized access, maintain data security, and correctly use the information we collect on-line.

VI. Parental Review of Information

Parents, please send a letter or postcard to our Privacy Manager at the mailing address provided below if you would like to do any of the following:

- access the personally identifiable information that the Neopets.com site has collected on-line from your child,
- correct factual errors in such information,
- request to have this information deleted, or
- request that we no longer collect or maintain such information.

Please be sure to include your e-mail address and a telephone number where we can reach you. To protect your child's privacy and security, we will take reasonable steps to help verify your identity before granting you access to the personal information that we collect and maintain about your child.

VII. Contact Us

If you have any questions, comments, or concerns regarding our privacy policy and/or practices, please contact us at the following e-mail address, address, and telephone number:

Privacy.Neopets@Neopets.com
Privacy Manager - Neopets.com
P.O. Box 10263
Glendale CA, 91209-0263
(818) 551 7580

If you are unable to resolve your concerns with our Privacy Manager, we encourage you to contact The Direct Marketing Association at www.the-dma.org.

VIII. A Final Note to Parents

The Internet offers a world of opportunity for children. Your guidance and involvement are essential to help ensure that children have a safe and rewarding on-line experience. We encourage you to visit The Direct Marketing Association's Web site (www.the-dma.org) and explore the Get CyberSavvy! program at <http://www.cybersavvy.org/cybersavvy/index.html>. Get CyberSavvy! helps families learn how information flows on-line so they can use the Internet in ways that protect their privacy and well-being. It also contains a number of valuable resources to help parents and children be aware of and express their preferences about information that is collected on-line and how it is used. Your efforts to instill responsible information practices will help steer

your children to age-appropriate sites and will go a long way toward ensuring that your children have enriching experiences on-line.

IX. Effective Date

The privacy policy set out above is effective as of September 1, 2004, and applies to all information previously obtained by Neopets. Neopets reserves the right to change its privacy policy at its sole discretion. Neopets' users will be informed of any such change by Neopets posting a new privacy policy on the neopets.com website. The effective date of any change of privacy policy will be clearly marked.

Appendix 3 – Facebook Privacy Policy

This policy is effective as of December 6, 2007.

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information.

Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

2. You should have access to the information others want to share.

There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com.

Safe Use of Facebook

For information for users and parents about staying safe on Facebook, [click here](#).

Facebook's Privacy Policy



Facebook's Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook, located at www.facebook.com and its directly associated domains (collectively, "Facebook" or "Website")

By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the site www.facebook.com and its directly associated domains. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

If you have questions or concerns regarding this statement, you should first contact our privacy staff at privacy@facebook.com . If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should contact TRUSTe Watchdog at http://www.truste.org/consumers/watchdog_complaint.php. TRUSTe will then serve as a liaison with us to resolve your concerns.

EU Safe Harbor Participation

We participate in the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce. As part of our participation in the safe harbor, we have agreed to TRUSTe dispute resolution for disputes relating to our compliance with the Safe Harbor Privacy Framework. If you have any complaints regarding our compliance with the Safe Harbor you should first contact us at info@facebook.com . If contacting us does not resolve your complaint, you may raise your complaint with TRUSTe at http://www.truste.org/users/users_watchdog_intro.html.

The Information We Collect

When you visit Facebook you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us.

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature.

When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information.

You post User Content (as defined in the Facebook Terms of Use) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is a violation of the Facebook Terms of Service and should be reported to privacy@facebook.com .

If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will automatically send your friend a one-time email or instant message inviting him or her to visit the site. Facebook stores this information to send this one-time invitation, to register a friend connection if your invitation is accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database.

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at info@facebook.com .

Children Between the Ages of 13 and 18

We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook

When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email address to send you notifications regarding new services offered by Facebook that we think you may find valuable.

Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network and those limited pieces of information may be made available to third party search engines. This is primarily so

your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

Facebook may send you service-related announcements from time to time through the general operation of the service. For instance, if a friend sends you a new message or poke, or someone posts on your wall, you may receive an email alerting you to that fact.

Generally, you may opt out of such emails from the Notifications page, though Facebook reserves the right to send you notices about your account even if you opt out of all voluntary email notifications.

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links).

Sharing Your Information with Third Parties

Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you. For example:

- Your News Feed and Mini-Feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your News Feed and Mini-Feed on your Privacy page.
- Unlike most sites on the Web, Facebook limits access to site information by third party search engine "crawlers" (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g. number of wall postings).
- We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the

processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.

- If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data. Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review these terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action.
- We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.
- We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.
- We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.
- We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.
- Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook discard that information, or to share it with your friends.

To learn more about the operation of the service, we encourage you to read the tutorial [here](#). To opt out of the service altogether, click [here](#).

Like many other websites that interact with third party sites, we may receive some information even if you are logged out from Facebook, or that pertains to non-Facebook

users, from those sites in conjunction with the technical operation of the system. In cases where Facebook receives information on users that are not logged in, or on non-Facebook users, we do not attempt to associate it with individual Facebook accounts and will discard it.

- If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this information may become publicly available.

Links

Facebook may contain links to other websites. We are of course not responsible for the privacy practices of other web sites. We encourage our users to be aware when they leave our site to read the privacy statements of each and every web site that collects personally identifiable information. This Privacy Policy applies solely to information collected by Facebook.

Third Party Advertising

Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about where individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them.

This privacy policy covers the use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers.

Changing or Removing Information

Access and control over most personal information on Facebook is readily available through the profile editing tools. Facebook users may modify or delete any of their profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., sending a personal message to another Facebook user) you generally cannot remove such communications.

Security

Facebook takes appropriate precautions to protect our users' information. Your account information is located on a secured server behind a firewall. When you enter sensitive information (such as credit card number or your password), we encrypt that information using secure socket layer technology (SSL). (To learn more about SSL, go to http://en.wikipedia.org/wiki/Secure_Sockets_Layer). Because email and instant messaging are not recognized as secure communications, we request that you not send private information to us by email or instant messaging services. If you have any questions about the security of Facebook Web Site, please contact us at privacy@facebook.com

Terms of Use, Notices and Revisions

Your use of Facebook, and any disputes arising from it, is subject to this Privacy Policy as well as our Terms of Use and all of its dispute resolution provisions including arbitration, limitation on damages and choice of law. We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's new effective date. If we make material changes to this policy, we will notify you here, by email, or through notice on our home page. We encourage you to refer to this policy on an ongoing basis so that you understand our current privacy policy. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account.

Contacting the Web Site

If you have any questions about this privacy policy, please contact us at privacy@facebook.com . You may also contact us by mail at 156 University Avenue, Palo Alto, CA 94301.