

29^E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

P R I V A C Y H O R I Z O N S

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Séance plénière

Dragon : *La prochaine génération*

La protection en ligne de la vie
privée des enfants

Plenary

“*The Next Generation*” Dragon
Children’s Online Privacy

27 septembre/September 27

10h45 – 12h

Série Terra Incognita, cahier de travail # 10/Terra Incognita, workbook series # 10

Table des matières / Table of contents

Biographies		Biographies	
M. Francesco Pizzetti — Président	2	Mr. Francesco Pizzetti — Chair	2
M ^{me} Jacquelyn Burkell, Ph. D.	2	Dr. Jacquelyn Burkell	2
M ^{me} Leslie Regan Shade, Ph. D.	3	Dr. Leslie Regan Shade	3
M ^{me} Valerie Steeves, Ph. D.	3	Dr. Valerie Steeves	3
Protection en ligne de la vie privée des enfants — Considérations stratégiques	5	Children’s Online Privacy — Policy Concerns	5

Biographies

Président : M. Francesco Pizzetti

Francesco Pizzetti est président de l'autorité italienne de protection des données. Il est professeur titulaire de droit constitutionnel à la faculté de droit de l'Université de Turin, professeur au campus Link de l'Université de Malte à Rome, et a aussi enseigné dans d'autres universités italiennes. Il a été conseiller en droit public administratif et constitutionnel auprès du gouvernement italien (1987-2001) et adjoint au maire de Turin (1990-1993). Il a également exercé diverses fonctions au gouvernement dans le cadre de plusieurs conférences et commissions et a été directeur de l'École supérieure d'administration publique italienne de 1998 à 2001. Il est membre du Conseil de la présidence de la justice administrative italienne et du conseil d'administration de l'Association italienne de droit constitutionnel. Par ailleurs, M. Pizzetti a effectué des recherches approfondies dans le domaine du droit constitutionnel italien et européen et s'est consacré plus particulièrement à l'étude de la réforme constitutionnelle de la République italienne, du fédéralisme italien et de l'élaboration d'un système complexe de gouvernance au sein du cadre institutionnel et de l'ordre juridique européens. Il est aussi auteur de plusieurs ouvrages et articles sur le droit constitutionnel et la réforme administrative.

Conférencières

M^{me} Jacquelyn Burkell, Ph. D.

Jacquelyn Burkell est professeure agrégée de la Faculté des études sur les médias et l'information de l'Université Western de l'Ontario. Elle est titulaire d'un doctorat en psychologie cognitive et ses intérêts en recherche portent notamment sur les implications sociales de la technologie. En collaboration avec Valerie Steeves et de nombreux autres partenaires de recherche, elle travaille actuellement à une Initiative de la nouvelle économie (INÉ) du Conseil de recherches en sciences humaines (CRSH), laquelle examine l'incidence de la technologie sur la vie privée. Elle donne des cours sur la technologie dans le cadre du programme sur les médias, l'information et la technoculture qui traite des nouvelles technologies et de notre interaction avec elles.

Biographies

Chair : Mr. Francesco Pizzetti

Francesco Pizzetti is President of the Italian data protection authority. He is Full Professor of Constitutional Law at the University of Turin's Faculty of Law, Professor at the Link University of Malta in Rome and has held academic offices at other Italian universities. He advised Italian governments on constitutional law and public administrative law (1987-2001), and served as deputy-mayor of Turin (1990- 1993). He has also served the government on several conferences and commissions and was Director of the Italian Superior School of Public Administration from 1998 to 2001. He is a member of the Council of the Presidency of the Italian Administrative Judiciary and a member of the Board of Directors of the Italian Association of Constitutional Law. He has performed extensive research on Italian and European Constitutional Law, concentrating on Italian Constitutional Reform, federalism, and developing a complex system of governance within the European framework and legal order. He has also written several books, papers and articles on constitutional law and administrative reform.

Speakers

Dr. Jacquelyn Burkell

Jacquelyn Burkell is a member in the Faculty of Media and Information Studies at the University of Western Ontario. She holds a PhD in Cognitive Psychology, and her research interests include the social implications of technology. She is currently involved in a SSHRC-INE, along with Val Steeves and many other research partners, that examines the impact of technology on privacy. Ms. Burkell teaches courses on technology in the Media, Information, and Technoculture program that examine new technologies and our interactions with them.

M^{me} Leslie Regan Shade, Ph. D.

Leslie Regan Shade est professeure agrégée au Département de communication de l'Université Concordia. Depuis le milieu des années 1990, ses recherches se concentrent sur les aspects sociaux, politiques et éthiques des technologies de l'information et des communications (TIC) et témoignent d'un intérêt particulier pour les questions liées au genre, à la mondialisation et à l'économie politique. Ses contributions à la recherche s'adressent à la fois aux universitaires et aux non-universitaires, y compris les décideurs et les groupes à but non lucratif. M^{me} Shade était la chercheuse principale d'un projet financé par le Conseil de recherches en sciences humaines, lequel examinait l'utilisation d'Internet par les enfants et les jeunes à la maison.

M^{me} Valerie Steeves, Ph. D.

Valerie Steeves est professeure adjointe au Département de criminologie et à la Faculté de droit (Section de common law) de l'Université d'Ottawa. Elle a rédigé de nombreux articles et fait de nombreux exposés sur la protection de la vie privée dans le contexte des droits de la personne et participe activement au processus d'élaboration de politiques en matière de protection de la vie privée au Canada. Elle a également rédigé plusieurs rapports sur l'utilisation des nouveaux médias par les enfants, y compris le rapport intitulé *Les jeunes Canadiens dans un monde branché* (Réseau Éducation-Médias, 2005). Elle est l'auteure d'une série de jeux multimédias visant à apprendre aux enfants à protéger leurs droits dans un environnement connecté. En 1999, elle a remporté le premier prix d'excellence annuel de la Fondation canadienne des relations raciales pour son jeu *Sense and NonSense* et, en 2006, elle a gagné la médaille de bronze pour son jeu *Privacy Playground* dans le cadre du Summit Creative Awards Competition, un concours international auquel prennent part des milliers de participants provenant de 26 pays. En 2004, elle a reçu le prix de conférence LaBelle de l'Université McMaster, un prix décerné aux universitaires qui font preuve d'avant-gardisme et remettent en question les idées reçues.

Dr. Leslie Regan Shade

Leslie Regan Shade is an Associate Professor at Concordia University in the Department of Communication Studies. Her research focus since the mid-1990's has been on the social, policy, and ethical aspects of information and communication technologies (ICTs), with particular concerns towards issues of gender, globalization, and political economy. Her research contributions straddle the line between academic and non-academic audiences, including policymakers and non-profit groups. Dr. Shade was the Principal Investigator for a Social Science and Humanities Research Council-funded project that looked at domestic use of the internet in the home for children and youth.

Dr. Valerie Steeves

Valerie Steeves is an Assistant Professor in the Department of Criminology and the Faculty of Common Law at the University of Ottawa. Dr. Steeves has written and spoken extensively on privacy from a human rights perspective, and is an active participant in the privacy policy making process in Canada. She has also written a number of reports on children's use of new media, including *Young Canadians in a Wired World* (Media Awareness Network, 2005), and is the author of a series of multimedia games designed to teach children how to protect their human rights in a networked environment. Her game *Sense and NonSense* won the first annual Award of Excellence in Race Relations Education from the Canadian Race Relations Foundation in 1999, and her game *Privacy Playground* won the Bronze Medal at the 2006 Summit Creative Awards Competition, an international competition involving thousands of entries from 26 countries. In 2004, she was awarded the LaBelle Lectureship at McMaster University, a juried prize given to scholars doing cutting edge research and challenging accepted ideas.

29^E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

P R I V A C Y H O R I Z O N S

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Protection en ligne de la vie privée des enfants
Considérations stratégiques

Children's Online Privacy
Policy Concerns

Par/by:

Valerie Steeves

Ce rapport propose un bref aperçu des préoccupations que soulève la protection de la vie privée des enfants sur Internet et dont il serait bon de tenir compte dans les politiques. Je commencerai par étudier les raisons ayant conduit à la promulgation de la *Children's Online Privacy Protection Act of 1998* des États-Unis, puis j'examinerai certaines des critiques émises dans la littérature à propos de la Loi (et du régime de protection des données sur lequel elle se base). Je présenterai enfin certaines des conclusions des recherches concernant les attitudes et les comportements au sujet de la protection de la vie privée des enfants et le rôle qu'elle joue dans le développement des enfants.

La thèse que je défends est que le cadre législatif actuel, qui repose sur des pratiques équitables de traitement de l'information censées donner aux enfants (et aux parents) un droit de regard sur la collecte et l'utilisation des données personnelles des enfants, peut ne pas suffire à protéger la vie privée des enfants sur Internet pour deux raisons. Premièrement, il ne prend pas en compte la dimension sociale des activités des enfants sur Internet. Deuxièmement, il n'endigues pas les impératifs commerciaux qui poussent à la commercialisation d'espaces de jeux privés à destination des enfants. Ironiquement, ces deux facteurs se combinent pour justifier une diminution plus importante du droit à la vie privée des enfants afin de mieux les protéger contre des pratiques agressives ou des contenus choquants. Afin d'éviter ces pièges, les politiques doivent reconnaître que les pratiques équitables de traitement de l'information représentent des mesures minimums et non maximums, et doivent fournir des mécanismes supplémentaires qui limitent l'exploitation commerciale des sites Web destinés aux enfants et garantissent que les besoins en matière de vie privée nécessaires au développement des enfants sont respectés par les sites Web.

Limiter les supercheries du Web (*Web of Deception*) – Mise en application de la *Children's Online Privacy Protection Act of 1998*

La protection de la vie privée des enfants sur Internet a été évoquée pour la première fois en termes de problème politique en 1996, lors de la publication, par l'organisme américain Center for Media Education (CME), d'un rapport appelé *Web of Deception: Threats to Children from Online*

This paper provides a brief overview of the policy concerns that have been raised concerning children's online privacy. I start by examining the impetus for enacting the *Children's Online Privacy Protection Act of 1998*, and then examine some of the criticisms of the Act (and the data protection regime upon which it is based) that have been raised in the academic literature. I then outline some of the research findings regarding children's privacy attitudes and behaviours, and the role that privacy plays in children's development.

I argue that the current legislative framework, which relies on fair information practices to give children (and parents) control over the collection and use of children's personal information, may be insufficient to protect children's online privacy for two reasons. First, it fails to take into account the social meaning of children's online activities. Second, it does not constrain the business imperatives that drive the commercialization of children's private play spaces. Ironically, these two factors combine to legitimize a further reduction in children's privacy in order to protect them from invasive practices and offensive content. In order to avoid these pitfalls, policy solutions must recognize that fair information practices are a floor rather than a ceiling, and provide additional mechanisms that limit the commercial exploitation of children's online spaces and ensure that children's developmental needs for privacy are respected in online spaces.

Restraining the *Web of Deception* – The Introduction of the *Children's Online Privacy Protection Act of 1998*

Children's online privacy was first raised as a policy issue in 1996, when the U.S.-based Center for Media Education (CME) released its report, *Web of Deception: Threats to Children from Online Marketing* (Montgomery, 1996). The report documented a number of marketing practices embedded in web sites designed for children, including the seamless blending of advertising with content, and the aggressive collection of children's personal information for commercial purposes. The information collected was used to micro-target individual children with advertising, and to develop detailed profiles of children as consumers. Collection was also masked as "play" – kids were encouraged to provide personal information in order to join a club or enter a contest – and the fact that the playground was created as a tool for market research was invisible to the users.

Marketing (Montgomery, 1996). Ce rapport faisait la liste d'un certain nombre de pratiques commerciales intégrées dans des sites Web à destination des enfants, comprenant le mélange de publicités avec du contenu et la collecte agressive de renseignements personnels auprès des enfants à des fins commerciales. Les renseignements recueillis étaient utilisés pour cibler individuellement les enfants avec des publicités et pour élaborer des profils détaillés d'enfants en tant que consommateurs. La collecte était déguisée en « jeux » - les enfants étaient encouragés à fournir des renseignements personnels pour faire partie d'un club ou participer à un concours – et le fait que le site de jeu était un outil de recherche commerciale était indétectable pour les utilisateurs.

Le CME déclarait que ces éléments constituaient des pratiques commerciales trompeuses et réclamait l'interdiction :

1. de la collecte d'informations personnelles auprès des enfants (y compris les données sur le parcours d'un internaute);
2. des liens entre des pages de contenu et des pages publicitaires;
3. de toute activité au cours de laquelle les enfants « parlent » à des personnages emblématiques de produits;
4. d'études commerciales en ligne microciblées ou à réponses directes visant des enfants.

Conscient de l'incapacité des enfants de faire la différence entre la publicité et les autres contenus, le CME demandait également aux spécialistes du marketing de signaler clairement les publicités.

Le Congrès américain a réagi rapidement et, après une série d'audiences, il a promulgué la *Children's Online Privacy Protection Act of 1998* (COPPA). La COPPA exige que les sites « à destination des enfants » obtiennent un consentement parental vérifiable pour la collecte d'informations auprès d'enfants de moins de 13 ans. Afin que ce consentement soit « vérifiable », l'exploitant du site Web doit prendre des mesures raisonnables pour s'assurer que les parents sont avertis des pratiques du site concernant le recueil d'informations et qu'ils y consentent. La méthode la plus simple est d'afficher sur le site une « mise en garde contre la divulgation d'informations personnelles ». La mise en garde doit préciser quelles informations sont recueillies et dans quel but, si les informations

The CME argued that these constituted deceptive trade practices and called for a ban on:

1. Collecting children's personal information (including clickstream data);
2. Hypertext links between content pages and advertising pages;
3. Any interactivity in which children "talk" to product spokes-characters;
4. Online micro-targeting or direct-response marketing involving children.

Concerned that young children cannot differentiate advertising from other content, the CME also called upon marketers to clearly label any advertising as such.

The U.S. Congress was quick to respond and, after a series of Congressional hearings, it passed the *Children's Online Privacy Protection Act of 1998* (COPPA). COPPA provides that sites "directed to children" must seek verifiable parental consent for collection of information from children under the age of 13. In order to be "verifiable", the site operator must take reasonable steps to ensure that the parent receives notice of—and consents to—the site's information practices. The primary method of doing this is through a Privacy Notice posted on the site. The Notice must stipulate what information is collected and for what purposes, whether the information will be disclosed to third parties, how the information is secured, and how to contact the site operator for access to the information or to request the information be deleted. Children 13 and over are deemed to be competent to consent on their own behalf.

The procedural protections contained in COPPA were modelled on the general data protection regimes in place elsewhere, and accordingly children's personal information enjoys some level of protection in the more than 40 jurisdictions that have passed privacy laws to date. However, it is interesting that early in the U.S. legislative process, the broader concerns raised by the CME about the commercialization of children's online play receded as reform efforts focused on the narrower questions of access, security and consent.

The protections offered by COPPA have been criticized for a number of reasons. Site operators are only required to comply with the Act if they have actual knowledge that a user is under 13, and many rely on a blank statement that the site is not intended for use by children to avoid responsi-

sont susceptibles d'être transmises à de tierces parties, comment les informations sont sécurisées et comment entrer en contact avec l'exploitant du site Web pour accéder aux informations ou réclamer leur suppression. Les enfants de 13 ans ou plus sont censés être suffisamment responsables pour donner leur consentement de leur propre initiative.

Les protections procédurales présentes dans la COPPA ont été copiées des régimes généraux de protection des données existant ailleurs et, par conséquent, les informations personnelles des enfants sont protégées jusqu'à un certain point dans plus de 40 États ayant édicté des lois sur la protection de la vie privée à ce jour. Cependant, il est intéressant de constater que, très tôt dans la procédure législative américaine, les inquiétudes plus générales soulevées par le CME au sujet de la commercialisation des jeux en ligne à destination des enfants ont été éclipsées du fait de la concentration des efforts de réforme sur la limitation de l'accès, la sécurité et le consentement.

Les protections offertes par la COPPA ont fait l'objet de diverses critiques. Les exploitants de sites ne sont obligés de se plier à la Loi que s'ils savent avec certitude avoir des utilisateurs de moins de 13 ans, et un grand nombre d'exploitants se contentent d'une déclaration laconique selon laquelle le site n'est pas conçu pour les enfants, afin d'éviter toute responsabilité (Hertzel, 2000, p. 443). Cela pose un problème, surtout quand on sait que les enfants préfèrent fréquenter les sites conçus pour les adultes (Burkell et Steeves, à paraître). Un grand nombre des processus mis en place pour vérifier le consentement parental par télécopie, numéro de téléphone sans frais ou courriel sont peu pratiques et trop compliqués (Grimes et Shade, 2005, p. 191), et il est malaisé de réprimer la non-conformité à la loi, car il est difficile de détecter les violations (Hertzel, 2000, p. 443). Pour couronner le tout, certains enfants déclarent qu'ils mentent tout simplement à propos de leur âge ou qu'ils donnent une fausse adresse électronique parentale pour obtenir l'autorisation d'accéder à un site (Media Awareness Network, 2004).

Les politiques de protection de la vie privée sur les sites fréquentés par les enfants peuvent également faire l'objet de critiques. La quasi-totalité d'entre elles sont difficiles à trouver, longues et rédigées d'une manière peu

bility (Hertzel, 2000, p. 443). This is particularly problematic given the evidence that children prefer to frequent sites that are designed for adults (Burkell & Steeves, forthcoming). Many of the processes in place to verify parental consent by fax, toll free telephone lines or email are inconvenient and unwieldy (Grimes & Shade, 2005, p. 191), and policing non-compliance is difficult as it is hard to detect violations (Hertzel, 2000, p. 443). In addition, some children tell us that they simply lie about their age or provide a false parental e-mail address in order to gain access to a site (Media Awareness Network, 2004).

Privacy policies on the sites kids visit are also open to criticism. Almost all of them are hard to find, long, and written at a reading level that makes them difficult for children – and many adults – to understand (Burkell & Steeves, forthcoming). Children report that they are unlikely to read policies because they are long and boring (Media Awareness Network, 2001, 2004), and when they do read them, they complain that the legal language and the complex structure are intended to take advantage of them because they do not read at a university level (Burkell, Steeves & Micheti, 2007, p. 24). But perhaps most troubling is that data protection legislation like COPPA has done little to curtail the burgeoning trade in children's information. Detailed dossiers on a million pre-schoolers, with names and addresses, for example, can be purchased for as little as \$5.00 (U.S.) (Electronic Privacy Information Center, 2003).

Child as Commodity

One of the most compelling criticisms of the current regime is that its focus on personal information neglects the fact that aggregate statistics can be used to invade online privacy. Aggregate profiles, created by pooling massive amounts of personal information, are used to subdivide online users, including children, into clearly defined audiences so access to them as individuals can be sold to advertisers (Estrin, 2007, p. 2).

This kind of micro-marketing does more than just deliver advertising. Sites aggressively collect information from children both directly and by recording their movements, interactions and discussions with others, then use that information to develop an intimate relationship between the child and the marketer (Chung & Grimes, 2005, p. 527). Marketers play upon children's developmental

compréhensible pour des enfants et pour un grand nombre d'adultes (Burkell et Steeves, à paraître). Les enfants déclarent qu'ils sont peu enclins à lire ces politiques qu'ils trouvent longues et ennuyeuses (Media Awareness Network, 2001, 2004) et quand ils les lisent, ils se plaignent que le vocabulaire juridique et la structure complexe sont faits pour les embrouiller, puisqu'ils n'ont pas les études nécessaires pour comprendre ce qu'ils lisent (Burkell, Steeves et Micheti, 2007, p. 24). Mais le plus inquiétant est que les lois sur la protection des données telles que la COPPA n'ont guère réussi à freiner le commerce florissant des informations concernant les enfants. Par exemple, on peut acheter pour seulement 5 \$US des dossiers détaillés sur un million d'enfants d'âge préscolaire, avec leurs noms et leurs adresses (Electronic Privacy Information Center, 2003).

L'enfant-marchandise

L'une des critiques les plus convaincantes du régime actuel est qu'il se concentre sur les informations personnelles et néglige le fait que des statistiques globales peuvent aussi être utilisées pour envahir la vie privée sur Internet. Des profils globaux, créés à partir de sondages pratiqués sur un nombre important d'internautes, sont utilisés pour segmenter les utilisateurs d'Internet, y compris les enfants, en cibles clairement définies dont l'accès peut être vendu à des publicitaires (Estrin, 2007, p. 2).

Ce type de micromarketing va plus loin que simplement diffuser de la publicité. Les sites recueillent agressivement des informations auprès des enfants à la fois directement et en enregistrant leurs mouvements, leurs interactions et leurs discussions avec d'autres enfants, puis en utilisant ces informations pour créer des relations proches entre les enfants et l'expert en marketing (Chung et Grimes, 2005, p. 527). Les experts en marketing jouent sur le besoin, naturel dans le développement des enfants, d'expérimenter des rôles, de communiquer avec leurs pairs, de prendre des risques et de rechercher des conseils sur des problèmes importants pour eux afin de les encourager à révéler des informations personnelles (Steeves, 2006; Youn, 2005). Ensuite, ils utilisent ces informations pour créer une relation entre l'enfant et la marque et pour manipuler le sentiment d'identité de l'enfant pour le rendre plus réceptif aux messages d'achats (Steeves, 2006; Linn, 2004).

needs to experiment with roles, communicate with peers, take risks, and seek advice on issues that are important to them, in order to encourage children to reveal information about themselves (Steeves, 2006; Youn, 2005). They then use that information to create a relationship between the child and the brand, and to manipulate the child's sense of identity to make him or her more amenable to purchasing messages (Steeves, 2006, Linn, 2004).

To fully protect children's privacy in the online environment, we must acknowledge the ways in which aggregate information can be used to manipulate individual behaviour (Shade, Porter & Sanchez, 2005; Grimes & Shade, 2005; U.S. Public Interest Research Group & Center for Digital Democracy, 2007). The crux of the issue is that the marketing system rests on surveillance. As marketing guru Rob Graham puts it, "There's no way to sugar coat this. In order to learn more about individual consumers, marketers have to resort to 'spying'" (Graham, 2006, cited in Estrin, 2007, p. 4). Information that is collected about individual children in this way may or may not be associated with the child's name; however, it is funnelled into a system that categorizes unique individuals according to patterns of behaviour they share with others. Based on that categorization, the individual child is not just targeted with advertising when he or she returns to the site, but is "re-targeted" – in other words, the marketer feeds the child information in order to *change his or her behaviour*. As one marketing expert puts it:

The beauty of [behavioural targeting] is that it allows publishers and advertisers to learn more about their customers not as group, but as individuals. Rather, than sifting through mountains of data meant to encapsulate the buying patterns of groups of people, [behaviour targeting is] a way to look into the minds of a single, potential customer (Estrin, 2007, p. 1).

In this system, the child becomes the commodity that is sold to advertisers: "Instead of selling a media product itself, [an online playground] is selling information about the children and young adults who are its fans" (Seiter, 2004, p. 98).

A growing number of commentators are questioning whether or not the current privacy regime, with its emphasis on transparency and consent, is capable of protecting children in this environment

Afin de protéger complètement la vie privée des enfants dans l'environnement d'Internet, nous devons reconnaître les moyens utilisés pour manipuler le comportement individuel à partir d'informations globales (Shade, Porter et Sanchez, 2005; Grimes et Shade, 2005; U.S. Public Interest Research Group et Center for Digital Democracy, 2007). Le nœud du problème est que le système de marketing repose sur la surveillance rapprochée. Comme le dit le gourou du marketing Rob Graham : [Traduction] « il n'y a pas moyen d'enrober les choses : les experts en marketing doivent recourir à l'espionnage pour en savoir plus sur chaque consommateur » (Graham, 2006, cité dans Estrin, 2007, p. 4). Les informations personnelles recueillies de cette manière auprès des enfants peuvent ou non être associées au nom des enfants; cependant, elles passent dans un système qui segmente les personnes en fonction de leurs schémas de comportement. Sur la base de cette segmentation, l'enfant n'est pas simplement la cible de messages publicitaires lorsqu'il revient sur le site, il est « reciblé », c'est-à-dire que les experts en marketing lui donnent des informations susceptibles de *changer son comportement*. Comme le dit un expert en marketing :

[Traduction]

La beauté du [ciblage comportemental] réside dans le fait qu'il permet aux diffuseurs et aux publicitaires d'en savoir plus sur leurs clients non pas en tant que groupe, mais en tant que personne. Plutôt que de trier des montagnes de données conçues pour cerner les comportements d'achats de groupes de personnes, [le ciblage comportemental est] un moyen de pénétrer l'esprit d'un seul client potentiel. (Estrin, 2007, p. 1)

Dans ce système, l'enfant devient une marchandise vendue aux publicitaires : [Traduction] « au lieu de vendre un produit médiatique, [un site de jeux en ligne] vend des informations sur les enfants et les jeunes adultes qui le fréquentent » (Seiter, 2004, p. 98).

Un nombre croissant de commentateurs s'interrogent sur la capacité du régime actuel de protection de la vie privée, qui insiste sur la transparence et le consentement, à réellement protéger les enfants dans un tel environnement (Livingstone, 2003). La recherche montre qu'il est difficile, en particulier pour les jeunes enfants, de

(Livingstone, 2003). Research indicates that it is difficult for young children in particular to understand questions about privacy and the consequences of disclosure (Shade, Porter & Sanchez, 2004). Children are also much more likely to reveal personal information in exchange for a gift or benefit, without fully recognizing the reasons why the information is sought (Turow, 2001; Cai & Gantz, 2000). Moreover, they are often not given any real choice; children who do not wish to register or provide personal information for access to services like Hotmail or Instant Messaging are told simply not to use the service (Steeves, 2006). Many children report that, in those circumstances, they just press 'click' and accept whatever terms of service are imposed on them, whether they like it or not (Burkell, Steeves & Micheti, 2007).

To ensure we fully protect children's privacy, it is essential that policy makers take into account the commercial imperatives that drive information collection. As Chung and Grimes warn:

While it may be more difficult to imagine knowledge of children's play habits and social interactions as a highly valuable commodity, the reality of the \$115-billion children's consumer market and the massive revenues collected by children's marketers research play in the relationship that exists between children playing online and the continued growth of children's commercialized entertainment is crucial to understanding the consequences of the processes that unfold within the children's digital playground (Chung & Grimes, 2005, p. 541-542).

Child as Victim

One of the reasons that it has been difficult to restrict the commodification of children's online privacy is that policy makers often see the problem as a safety issue (Hertzell, 2000). From this perspective, the interactive nature of the Internet puts kids at increased risk of being watched by pedophiles and other ill-intentioned "strangers". Qualitative research with children indicates that the stranger-danger message has been communicated effectively (Livingstone & Bober, 2003, 2004; Media Awareness Network, 2004). As one child in Toronto put it, the rules are clear: "No porn, no chat, no personal information" (Media Awareness Network, 2004).

comprendre les enjeux relatifs à la protection de la vie privée et les conséquences de la divulgation d'informations (Shade, Porter et Sanchez, 2004). Les enfants sont également beaucoup plus enclins à révéler des informations personnelles en échange d'un cadeau ou d'un avantage, sans réaliser complètement les raisons pour lesquelles on leur demande ces informations (Turow, 2001; Cai et Gantz, 2000). De plus, ils n'ont pas souvent le choix; les enfants qui ne souhaitent pas s'enregistrer ou divulguer des informations personnelles pour accéder à certains services comme Hotmail ou des services de messagerie instantanés se voient tout simplement interdire l'accès à ces services (Steeves, 2006). De nombreux enfants déclarent que, dans ce cas, ils obtempèrent tout simplement et acceptent n'importe quelles conditions de service qu'on leur impose, que cela leur plaise ou non (Burkell, Steeves et Micheti, 2007).

Pour protéger complètement les enfants, il est essentiel que les personnes chargées d'élaborer les politiques tiennent compte des impératifs commerciaux qui président à la collecte d'information. Ainsi que Chung et Grimes nous en avertissent :

[Traduction]

Même s'il est difficile d'imaginer que la connaissance des habitudes de jeu et des interactions sociales des enfants soient une marchandise de valeur, la réalité du marché de la consommation des enfants, représentant 115 milliards de dollars, et les bénéfices massifs générés par les études de marché auprès des enfants jouent un rôle dans les relations existant entre les enfants qui jouent en ligne et la croissance constante des jeux exploités à des fins commerciales; il est crucial de comprendre les processus qui se développent sur le terrain des jeux virtuels à destination des enfants (Chung et Grimes, 2005, p. 541-542).

L'enfant-victime

L'une des raisons pour lesquelles il a été difficile de restreindre la marchandisation de la vie privée des enfants sur Internet vient de ce que les personnes chargées d'élaborer les politiques considèrent qu'il s'agit d'un problème de sécurité (Hertzfel, 2000). De ce point de vue, la nature interactive d'Internet augmente les risques pour

Ironiquement, le désir de protéger children from "strangers" has had the paradoxical effect of placing children under increased online surveillance. Commercial sites have tended to equate privacy risks with safety, teaching kids to guard their personal information from "strangers." However, kids are encouraged to reveal information to marketers and corporations. For example, Neopets.com, the premier children's marketing research site on the Web¹, warns kids not to give out personal information to other children on the site or to "strangers" on the Net. The site also encourages kids to report any suspicious activity so Neopets can "take any necessary action" to protect them². In this sense, the corporation purports to be part of the solution, rather than part of the problem, and commercial surveillance is normalized.

For their part, parents are encouraged to use key capture software and other technical "fixes" so they can see exactly what their children are doing online, in order to "keep them safe"³. Some commentators warn that these kinds of approaches tend to breed fear and suspicion, and make it more difficult for children to maintain relationships of trust with their parents and other adults (Livingstone, 2006). They may also be counter-productive. Kerr and Stattin (2000) report that increased parental monitoring of children does not correlate with a decrease in anti-social behaviour as previously reported; rather, children who spontaneously disclose information about their lives to their parents in the context of a relationship built on mutual trust are less likely to act in an anti-social manner.

The argument that we need to place children under surveillance to keep them safe also feeds into a "moral panic" about the dangers of the Internet (Lawson & Comber, 2000). The more fearful adults become, the harder it is to provide children with opportunities to enjoy privacy, which is essential to developing a healthy sense of autonomy (Tang & Dong, 2006). Schools are a case in point. Although the Internet is recognized as an outstanding curricular resource, many schools place students under virtual surveillance and threaten them with a loss of computer privileges if they violate the school's acceptable use policy (Lawson & Comber, 2000). The intent is to protect children from invasive behaviour on the part of others and to restrict their access to questionable content. However, this type of surveillance may backfire. Davis notes:

les enfants d'être observés par des pédophiles ou d'autres « étrangers » mal intentionnés. Une recherche qualitative effectuée auprès d'enfants montre que le message concernant les « étrangers » est passé efficacement (Livingstone et Bober, 2003, 2004; Media Awareness Network, 2004). Comme le souligne un enfant de Toronto, les règles sont claires : « pas de porno, pas de bavardage en ligne, pas d'informations personnelles » (Media Awareness Network, 2004).

Ironiquement, le désir de protéger les enfants contre les « étrangers » a eu un effet paradoxal, en plaçant les enfants sous une surveillance virtuelle accrue. Les sites commerciaux ont eu tendance à placer sur le même plan les risques concernant la vie privée et ceux concernant la sécurité, en enseignant aux enfants à préserver leurs informations personnelles des « étrangers ». Cependant, les enfants sont invités à révéler des informations aux experts en marketing et aux entreprises. Par exemple, Neopets.com, le premier site de recherches marketing d'Internet¹ sur les enfants, prévient les enfants de ne pas donner d'informations personnelles à d'autres enfants présents sur le site ou à des « étrangers » sur Internet. Le site incite aussi les enfants à signaler toute activité suspecte, afin que Neopets puisse « prendre toute mesure nécessaire » pour les protéger². Ainsi, la société est censée faire partie de la solution et non pas du problème, et la surveillance commerciale est présentée comme normale.

De leur côté, les parents sont invités à utiliser un logiciel de suivi des opérations et d'autres corrections techniques pour suivre exactement ce que font leurs enfants lorsqu'ils sont connectés, afin de les « protéger »³. Certains commentateurs avertissent que ce type d'approches peut entretenir la peur et la méfiance et rendre les relations de confiance entre les enfants et leurs parents et les autres adultes plus difficiles (Livingstone; 2006). Ces approches peuvent également être contre-productives. Kerr et Stattin (2000) relèvent qu'il n'existe pas de corrélation entre une surveillance parentale accrue des enfants et une baisse des comportements asociaux, comme on l'affirmait par le passé. Au contraire, les enfants qui ont tendance à donner spontanément à leurs parents des informations sur leur vie, dans le cadre de relations basées sur la confiance mutuelle, sont moins enclins à agir de manière asociale.

To discern and to 'own' appropriate connections and justifications requires a certain kind of 'privacy' from the teacher. That is, the teacher, as authoritative source of knowledge, needs to be distanced in some measure from the processes through which this discernment and ownership is acquired. In some measure the teacher must lack detailed access to the child's thinking processes, at least for some of the time, and *the child must be aware that the teacher lacks this access* (emphasis in original, Davis, 2001, pp. 252).

Blanket surveillance may then work against the best interests of children as it interferes with the learning process itself.

Child as Suspect

The use of online surveillance in schools as "some sort of scare tactic about being caught out" (Lawson & Comber, 2000, p. 281-282) may also impede the development of democratic sensibilities (Davis, 2001). A number of Canadian students who participated in focus groups in 2004 reported that they were afraid of pornographic pop-ups that appeared spontaneously on school computers—not because they did not know how to deal with the content, but because they would not be able to prove to teachers that they were "innocent" (MNet, 2004).

Giroux argues that children are "increasingly isolated, treated with suspicion, and subjected to diminished rights to privacy and personal liberties" (Giroux, 2003, p. 553), particularly in schools. He warns that zero tolerance policies (and acceptable use policies by extension) run the risk of criminalizing young people's behaviour and creating a "generation of suspects" (p. 554). Garrett (2004) has similar concerns about the increasing use of databases to monitor "troublesome" youth.

A number of commentators contend that children are now subjected to more surveillance than ever before (James & James, 2001), and that the use of monitoring has become "central characteristic of modern childhood" (Fotel, Thomsen, 2004, p. 535). In these circumstances, it is even more important to develop policies that protect children's privacy in the fullest sense.

L'argument selon lequel nous devons mettre l'enfant sous surveillance afin de le protéger contribue également à alimenter la « peur morale » à propos des dangers d'Internet (Lawson et Comber, 2000). Plus les adultes ont peur, plus il devient difficile de protéger la vie privée des enfants, qui est essentielle au développement d'un sens de l'autonomie solide (Tang et Dong, 2006). Les écoles sont un exemple typique. Alors qu'Internet est reconnu comme une ressource pédagogique remarquable, un grand nombre d'écoles placent les étudiants sous surveillance virtuelle et les menacent de perdre l'accès aux ordinateurs s'ils violent la politique d'utilisation acceptable de l'école (Lawson et Comber, 2000). L'intention première est de protéger les enfants contre les comportements envahissants de la part d'autres personnes et de limiter l'accès à des contenus discutables. Pourtant, ce type de surveillance peut se révéler contre-productif. Davis remarque que :

[Traduction]

Apprendre à discerner les connexions et les justifications appropriées et se les « approprier » réclame une dose de respect de la vie privée de la part du professeur. Cela signifie que le professeur, source reconnue de savoir, doit, dans une certaine mesure, être mis à l'écart des processus par lesquels ce discernement et cette appropriation seront acquis. Jusqu'à un certain point, le professeur doit se priver d'accéder de manière trop détaillée au processus de réflexion de l'enfant, en tout cas à certains moments, et *l'enfant doit avoir conscience que le professeur se prive de cet accès* (ce point est mis en évidence dans le document original, Davis, 2001, p. 252).

Une surveillance rapprochée peut donc aller à l'encontre des intérêts des enfants en interférant avec le processus d'apprentissage lui-même.

L'enfant-suspect

L'utilisation d'une surveillance en ligne dans les écoles comme « d'une sorte de stratégie de la peur d'être pris » (Lawson et Comber, 2000, p. 281 et 282) peut également entraver le développement du sens de la démocratie (Davies, 2001). Un grand nombre d'étudiants canadiens ayant participé à des groupes de réflexion en 2004 ont rapporté qu'ils craignaient les

Why Children's Privacy is Important

Understanding children's privacy attitudes and behaviours is an important piece of the policy puzzle, and yet policymakers to date have tended to ignore the impact of data protection policies on kids' experiences (Shade, Porter, Sanchez, 2005, p. 521). Early polls that indicated that children are willing to trade away personal information in order to win a prize or enter a contest (Turow, 2001; Media Awareness Network, 2000) led many to conclude that young people do not care about privacy. However, there is a growing body of research that indicates that children actively seek online privacy—but they seek it from their parents, their siblings, and their teachers (Livingstone, 2006; Livingstone & Bober, 2003, 2004; Media Awareness Network, 2004).

Children value their online privacy precisely because it gives them a safe space in which to try on new identities, experiment with social roles, communicate with peers, and get a glimpse of an adult world that is otherwise closed to them (Livingstone, 2006; Steeves, 2006). They move seamlessly between real world activities and online communication, often talking on the phone, doing homework online, chatting with friends on Instant Messaging and downloading music, all at the same time (Media Awareness Network, 2000). Rather than isolating them, the Net gives them a way to extend their real world social networks. Younger children often prefer online communication to face-to-face conversations or telephone calls because it is harder for others to overhear them. It also gives them a way to manage any potentially embarrassing situations as they can pretend they were kidding or otherwise “elegantly withdraw from the stage” in the Goffmanian sense (Livingstone & Bober, 2003, 2004).

Children also micro-manage their online privacy and actively resist parents' and teachers' surveillance (Livingstone & Bober, 2003, 2004; Hope, 2005). They liken adult cyber-snooping to having their pockets picked (Livingstone & Bober, 2003, 2004) or being stalked (Burkell, Steeves & Micheti, 2007). This is ironic, given that well-meaning adults often resort to these types of practices in order to protect their children's privacy from strangers.

On the other hand, children are often naive about corporate surveillance (Shade, Porter, & Sanchez, 2005), and can appear to passively accept it as a

fenêtres pornographiques qui peuvent apparaître soudainement sur les écrans des ordinateurs de l'école non pas parce qu'ils ne savaient pas comment y faire face, mais parce qu'ils savaient qu'ils ne pourraient pas prouver aux professeurs qu'ils étaient « innocents » (MNet, 2004).

Giroux déclare que les enfants sont de plus en plus isolés, soupçonnés et soumis à une restriction de leur droit à la protection de la vie privée et à la liberté personnelle (Giroux, 2003, p. 553), en particulier dans les écoles. Il met en garde contre les politiques de tolérance zéro (et par extension contre les politiques d'utilisation acceptable) qui font courir le risque de la criminalisation du comportement des jeunes et de la création d'une « génération de suspects » (p. 554). Garrett (2004) éprouve les mêmes craintes à propos de l'utilisation croissante de bases de données censées surveiller les jeunes « à problèmes ».

Un grand nombre de commentateurs affirment qu'aujourd'hui, les enfants sont plus surveillés qu'ils ne l'ont jamais été (James et James, 2001), et que l'utilisation de la surveillance est devenue « une caractéristique principale de l'enfance moderne » (Fotel, Thomsen, 2004, p. 535). Dans ces conditions, il est encore plus important de concevoir des politiques qui protègent la vie privée des enfants au sens le plus large du terme.

Pourquoi la protection de la vie privée des enfants est-elle importante

La compréhension des attitudes et des comportements inhérents à la protection de la vie privée des enfants est une pièce importante dans le puzzle de la politique sur la protection de la vie privée, mais, jusqu'à aujourd'hui, les personnes chargées de concevoir cette politique ont eu tendance à ignorer l'influence des politiques de protection des données sur les expériences des enfants (Shade, Porter, Sanchez, 2005, p. 521). Les premiers sondages, qui montraient que les enfants sont capables de donner des informations personnelles dans l'espoir de gagner un prix ou de participer à un concours (Turow, 2001; Media Awareness Network, 2000) ont conduit nombre de personnes à conclure que les jeunes ne se soucient pas de protéger leur vie privée. Cependant, de plus en plus d'études montrent que les enfants recherchent activement à protéger leur vie privée en ligne – mais qu'ils le font contre leurs parents, leurs frères et sœurs et leurs

fact of life (Burkell, Steeves & Micheti, 2007). Nonetheless, there is evidence that they are uncomfortable with the ways in which they are constantly monitored by online corporations. Although they routinely “click through” in order to get access to online games or communication platforms, many lament their lack of options. As a 15-year old Canadian girl puts it, “Like, if we had a choice to say no, I would choose no. We can't or else we can't go on the thing for some of them” (p. 14). Interestingly, this lack of options translates into a general distrust of the corporations that house the sites they visit. In the words of a 17-year old Canadian boy, “Well, they're taking advantage of you, that your friends have a Hotmail account, they're on Messenger, like you have to have Messenger... It's another way to control you” (*ibid*).

Although data protection laws offer some protection, policy makers have yet to fully accommodate the privacy needs of children. Privacy is an essential element of growing up. Online self-expression is linked to identity formation and a sense of self respect (Stern, 2004), and private online spaces give children an opportunity to develop a sense of autonomy (Livingstone, 2007). Children turn to the Net to fulfill age-appropriate developmental needs for individuation (Tang), and respecting their developmental need for privacy will encourage them to go beyond the acquisition of “thin” procedural skills and develop a facility for deeper, “connected thinking” (Davis, 2001, p. 252).

Clearly, to deny the existence of online risks to children's safety would be irresponsible (Livingstone, 2006). But at the same time, policy makers must address the ways in which children's online spaces are structured by pervasive surveillance. Current rules do little to restrict the commodification of children's private lives, and the ways in which children's privacy and freedom of expression is limited by organizations that turn them into objects of surveillance.

In order to find a better balance, fair information practices should be supplemented with regulations that limit behavioural targeting of children and immersive advertising in online playgrounds. Schools and libraries should be encouraged to provide children with privacy education, and restrictions on children's freedom of speech and access to information should be carefully fine-tuned to ensure children benefit from the democratic potential of online communication. Parents also need education and support to better guide

professeurs (Livingstone, 2006; Livingstone et Bober, 2003, 2004; Media Awareness Network, 2004).

Les enfants attachent de l'importance à leur vie privée en ligne justement parce que cela leur donne un espace sécurisé dans lequel ils peuvent essayer de nouvelles identités, faire l'expérience de nouveaux rôles sociaux, communiquer avec leurs pairs et jeter un coup d'œil sur le monde des adultes, qui leur serait fermé sans cela (Livingstone, 2006; Steeves, 2006). Ils évoluent continuellement entre les activités du monde réel et la communication en ligne, ils parlent au téléphone, ils font leurs devoirs en ligne, ils bavardent avec des amis sur les sites de messagerie instantanée et ils téléchargent de la musique, tout cela en même temps (Media Awareness Network, 2000). Loin de les isoler, Internet leur offre un moyen d'étendre leur réseau de relations dans le monde réel. Les plus jeunes enfants préfèrent souvent la communication en ligne aux conversations en face à face ou aux appels téléphoniques car, cette communication se prête moins aux intrusions. Cela leur offre également la possibilité de se tirer de situations potentiellement embarrassantes puisqu'ils peuvent prétendre qu'ils plaisaient ou « se retirer élégamment de la scène » au sens goffmanien du terme (Livingstone et Bober, 2003, 2004).

Les enfants microgèrent aussi leur vie privée en ligne et résistent activement à la surveillance des parents et des professeurs (Livingstone et Bober, 2003, 2004; Hope, 2005). Ils assimilent le fouinage virtuel des adultes à du vol à la tire (Livingstone et Bober, 2003, 2004) ou à du harcèlement (Burkell, Steeves et Micheti, 2007). C'est ironique, car les adultes bien intentionnés n'ont souvent recours à ce genre de pratiques que pour protéger la vie privée des enfants contre les étrangers.

D'un autre côté, les enfants sont souvent naïfs à propos de la surveillance pratiquée par les entreprises (Shade, Porter, et Sanchez, 2005), et ils donnent l'impression de l'accepter passivement comme un fait accompli (Burkell, Steeves et Micheti, 2007). Néanmoins, il existe des preuves qu'ils ne se sentent pas à l'aise quant à la surveillance permanente dont ils font l'objet par les entreprises. Même s'ils continuent par habitude à accepter les « clics publicitaires » pour accéder aux jeux en ligne ou aux plateformes de

their children's online activities.

Data protection commissioners have a special role to play in this process. As privacy experts, they can support an informed public debate about children's privacy. They can also provide valuable privacy expertise to governments and administrators who are responsible for managing various aspects of children's online communications. Data protection principles are an important part of that expertise, but commissioners can also seek to engage governments in a meaningful debate about the value of privacy to children's development and education. Most importantly, commissioners can reinvigorate the role of privacy as a human right, and seek to advance privacy as an essential element of human dignity and democratic freedom.

Works Cited

- Burkell, Jacquelyn, Valerie Steeves and Anca Micheti. (2007). *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand*. Ottawa: Privacy Commissioner of Canada.
- Burkell, Jacquelyn and Valerie Steeves. (Forthcoming.) *Reading the Fine Print: Assessing the Accessibility of Privacy Policies on Kids' Favorite Web Sites*.
- Cai, Xiaomei & Walter Gantz. (2000). Online Privacy Issues Associated with Web Sites for Children. *Journal of Broadcasting & Electronic Media* 44(2): 197-214.
- Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501-6506.
- Chung, Grace and Sara M. Grimes. (2005). Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games. *Canadian Journal of Communication* 30(4): 527-548.
- Davis, Andrew. (2001). Do Children Have Privacy Rights in the Classroom? *Studies in Philosophy and Education* 20: 245-254.
- Electronic Privacy Information Center. (2003). *The Children's Online Privacy Protection Act (COPPA)*. <http://www.epic.org/privacy/kids/>

communication, un grand nombre d'entre eux regrettent l'absence de choix. Comme le dit une jeune Canadienne de 15 ans : [Traduction] « par exemple, si j'avais le choix, je répondrais non. Mais nous n'avons pas cette possibilité ou alors on ne peut pas accéder à tout » (p. 14). Il est intéressant de noter que cette absence de choix se traduit par une défiance générale à l'encontre des sociétés qui accueillent les sites fréquentés par les jeunes. Dixit un jeune Canadien de 17 ans : [Traduction] « Bien, ils profitent de vous, de vos amis qui ont un compte Hotmail, ils sont sur Messenger donc vous devez avoir Messenger... c'est un moyen de vous contrôler » (*ibid*).

Même si les lois sur la protection des données offrent une certaine protection, il reste encore aux personnes chargées de concevoir les politiques à tenir compte complètement des besoins de protection de la vie privée des enfants. C'est un élément essentiel à une croissance harmonieuse. L'expression personnelle sur Internet est en relation avec la formation de la personnalité et la conscience de sa propre dignité (Stern, 2004), et des espaces virtuels privés offrent aux enfants la possibilité de développer leur autonomie (Livingstone, 2007). Les enfants utilisent Internet pour combler les besoins de développement liés à l'individuation appropriés à leur âge (Tang), et respecter leurs besoins de développement en terme de respect de leur vie privée les encouragera à aller au-delà de l'acquisition de compétences procédurales « légères » et à développer des compétences en termes de « pensée connectée » approfondie (Davis, 2001, p. 252).

Il est évident qu'il serait irresponsable de nier l'existence de risque pour les enfants sur Internet (Livingstone, 2006). Mais en même temps, les personnes chargées de concevoir les politiques doivent s'intéresser à la façon, basée sur une surveillance intense, de structurer les espaces virtuels destinés aux enfants. Les règles actuelles sont insuffisantes pour restreindre la marchandisation de la vie privée des enfants et la façon dont le respect de leur vie privée et leur liberté d'expression sont limitées par des organismes qui transforment les enfants en objets d'étude.

Afin de trouver un meilleur équilibre, les pratiques équitables de traitement de l'information doivent être complétées par des réglementations limitant

Estrin, Michael. (2007, April 20). *Behavioural Marketing – Getting Ads to the Right Eyeballs*. iMedia Connection. <http://www.imediaconnection.com/content/14559.asp>

Fotel, Trine and Thyra Uth Thomsen. (2004). The Surveillance of Children's Mobility. *Surveillance & Society* 1(4): 535-554.

Garrett, Paul Michael. (2004). The Electronic Eye: Emerging Surveillance Practices in Social Work with Children and Families. *European Journal of Social Work* 7(1): 57-71.

GetNetWise. (1999-2003). *Loss of Privacy*. <http://kids.getnetwise.org/safetyguide/danger/privacy>

Giroux, Henry A. (2003). Racial Injustice and Disposable Youth in the Age of Zero Tolerance. *Qualitative Studies in Education* 16(4): 553-565.

Graham, Rob. (2006). *Fishing from a Barrel – Using Behavioral Targeting to Reach the Right People with the Right Ads at the Right Time*. Boscawen, NH: Learningcraft Press.

Grimes, Sara and Leslie Regan Shade. (2005). Neopian Economics of Play: Children's Cybepets and Online Communities as Immersive Advertising in Neopets.com. *International Journal of Media and Cultural Politics* 1(2): 181-198.

Hertzel, Dorothy. (2000). Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online. *Federal Communications Law Journal* 52(2): 429-451.

Hope, Andrew. (2005). Panopticism, Play and the Resistance of Surveillance: Case Studies of the Observation of Student Internet Use in UK Schools. *British Journal of Sociology of Education* 26(3): 359-373.

James, A. L. & James, A. (2001). Tightening the Net: Children, Community and Control. *British Journal of Sociology* 52(2): 211-228.

Kerr, Margaret and Håkan Stattin. (2000). What Parents Know, How They Know It, and Several Forms of Adolescent Adjustment: Further Support for a Reinterpretation of Monitoring. *Devel-*

le ciblage comportemental des enfants et la publicité cachée dans les sites de jeux en ligne. Les écoles et les bibliothèques devraient être poussées à donner aux enfants des cours sur la protection de la vie privée, et les restrictions de la liberté de parole et de l'accès aux informations pour les enfants devraient être strictement mesurées pour leur garantir l'accès au potentiel démocratique des communications en ligne. Les parents ont également besoin d'informations et de soutien pour mieux guider leurs enfants dans leurs activités en ligne.

Les commissaires à la protection des données ont un rôle particulier à jouer dans ce processus. En tant qu'experts de la protection de la vie privée, ils peuvent encourager un débat public documenté sur la protection de la vie privée des enfants. Ils peuvent aussi fournir une expertise précieuse en matière de protection de la vie privée aux gouvernements et aux administrations, qui sont responsables de la gestion des divers aspects des communications virtuelles des enfants. Les principes de la protection des données représentent une part importante de cette expertise, mais les commissaires peuvent aussi essayer d'engager les gouvernements dans un débat fructueux sur la valeur de la protection de la vie privée des enfants en ce qui concerne leur développement et leur éducation. Plus important encore, les commissaires peuvent réaffirmer le rôle de la protection de la vie privée en tant que droit de la personne, et tenter de montrer la protection de la vie privée comme un élément essentiel de la dignité humaine et de la liberté démocratique.

Ouvrages cités

- Burkell, Jacquelyn, Valerie Steeves et Anca Micheti. (2007). *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand*. Ottawa: Commissariat à la protection de la vie privée du Canada.
- Burkell, Jacquelyn et Valerie Steeves. (À paraître.) *Reading the Fine Print: Assessing the Accessibility of Privacy Policies on Kids' Favorite Web Sites*.
- Cai, Xiaomei et Walter Gantz. (2000). Online Privacy Issues Associated with Web Sites for Children. *Journal of Broadcasting & Electronic Media* 44(2): 197-214.

omental Psychology 36(3): 366-380.

- Lawson, Tony and Chris Comber. (2000). Censorship, the Internet and Schools: a New Moral Panic? *The Curriculum Journal* 11(2): 273-285.
- Linn, S. (2004). *Consuming Kids: The Hostile Takeover of Childhood*. New York: The New Press.
- Livingstone, Sonia. (2006). Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. Computers, Phones, and the Internet: Domesticating Information Technology. Eds. Kraut, R. E., M. Brynin and S. Kiesler. New York: Oxford University Press.
- (2003). Children's Use of the Internet: Reflections on the Emerging Research Agenda. *New Media & Society* 5(2): 147-166.
- Livingstone, Sonia & Magdalena Bober. (2003). *UK Children Go Online: Listening to Young People's Experiences*. London: Economic and Social Research Council.
- (2004). *UK Children Go Online: Surveying the Experiences of Young People and their Parents*. London: Economic and Social Research Council.
- Media Awareness Network. (2004). *Young Canadians in a Wired World: Phase II Focus Groups*. Ottawa.
- (2000). *Parents and Youth Focus Groups, 2000*. Ottawa.
- Montgomery, Kathryn. (1996). *Web of Deception: Threats to Children from Online Marketing*. Washington: Center for Media Education.
- Neopets. Safety Tips at <http://www.neopets.com/safetytips.phtml>.
- Neopets. Privacy Policy at <http://www.neopets.com/privacy.phtml>
- Seiter, Ellen. (2004). The Internet Playground. *Toys, Games, and Media*. Eds. Jeffrey Goldstein, David Buckingham, and Gilles Brougère. Mahwah, NJ: Lawrence Erlbaum Associates.
- Shade, Leslie Regan, Nikki Porter and Wendy

- Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501-6506.
- Chung, Grace et Sara M. Grimes. (2005). Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games. *Canadian Journal of Communication* 30(4): 527-548.
- Davis, Andrew. (2001). Do Children Have Privacy Rights in the Classroom? *Studies in Philosophy and Education* 20: 245-254.
- Electronic Privacy Information Center. (2003). *The Children's Online Privacy Protection Act (COPPA)*. <http://www.epic.org/privacy/kids/>
- Estrin, Michael. (2007, 20 avril). *Behavioural Marketing – Getting Ads to the Right Eyeballs*. iMedia Connection. <http://www.imediaconnection.com/content/14559.asp>
- Fotel, Trine et Thyra Uth Thomsen. (2004). The Surveillance of Children's Mobility. *Surveillance & Society* 1(4): 535-554.
- Garrett, Paul Michael. (2004). The Electronic Eye: Emerging Surveillant Practices in Social Work with Children and Families. *European Journal of Social Work* 7(1): 57-71.
- GetNetWise. (1999-2003). *Loss of Privacy*. <http://kids.getnetwise.org/safetyguide/danger/privacy>
- Giroux, Henry A. (2003). Racial Injustice and Disposable Youth in the Age of Zero Tolerance. *Qualitative Studies in Education* 16(4): 553-565.
- Graham, Rob. (2006). *Fishing from a Barrel – Using Behavioral Targeting to Reach the Right People with the Right Ads at the Right Time*. Boscawen, NH: Learningcraft Press.
- Grimes, Sara et Leslie Regan Shade. (2005). Neopian Economics of Play: Children's Cyberpets and Online Communities as Immersive Advertising in Neopets.com. *International Journal of Media and Cultural Politics* 1(2): 181-198.
- Hertzell, Dorothy. (2000). Don't Talk to Strangers: An Analysis of Government and Industry Ef-
- Sanchez. (2005). "You Can See Anything on the Internet, You Can Do Anything on the Internet!": Young Canadians Talk About the Internet. *Canadian Journal of Communication* 30(4): 503-526.
- Steeves, Valerie. (2006). It's Not Child's Play: The Online Invasion of Children's Privacy. *University of Ottawa Law and Technology Journal* 3 (1): 169-188.
- Stern, Susannah R. (2004). Expressions of Identity Online: Prominent Features and Gender Differences in Adolescents' World Wide Web Home Pages. *Journal of Broadcasting & Electronic Media* 48(2): 218-243.
- Tang, Shengming and Xiaoping Dong. (2006). Parents' and Children's Perceptions of Privacy Rights in China. A Cohort Comparison. *Journal of Family Issues* 27(3): 285-300.
- Turow, J. (2001). *Privacy Policies on Children's Websites: Do They Play by the Rules?* Philadelphia: Annenberg Public Policy Centre of the University of Pennsylvania.
- US Public Interest Research Group and Center for Digital Democracy. (2006, November 1). *Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices*. Filed with the Federal Trade Commission.
- Youn, Seounmi. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media* 49 (1): 86-110.

Endnotes

¹ Neopets is available in 11 languages, including English, Spanish, German, French, Italian, Chinese Traditional, Chinese Simplified, Japanese, Korean, Dutch, and Portuguese.

² Neopets Safety Tips at <http://www.neopets.com/safetytips.phtml>.

See also, Neopets Privacy Policy at <http://www.neopets.com/privacy.phtml>.

Neopets is COPPA compliant.

³ See GetNetWise's Loss of Privacy page, for example, at <http://kids.getnetwise.org/safetyguide/danger/privacy>

- forts to Protect a Child's Privacy Online. *Federal Communications Law Journal* 52(2): 429-451.
- Hope, Andrew. (2005). Panopticism, Play and the Resistance of Surveillance: Case Studies of the Observation of Student Internet Use in UK Schools. *British Journal of Sociology of Education* 26(3): 359-373.
- James, A. L. et James, A. (2001). Tightening the Net: Children, Community and Control. *British Journal of Sociology* 52(2): 211-228.
- Kerr, Margaret et Håkan Stattin. (2000). What Parents Know, How They Know It, and Several Forms of Adolescent Adjustment: Further Support for a Reinterpretation of Monitoring. *Developmental Psychology* 36(3): 366-380.
- Lawson, Tony et Chris Comber. (2000). Censorship, the Internet and Schools: a New Moral Panic? *The Curriculum Journal* 11(2): 273-285.
- Linn, S. (2004). *Consuming Kids: The Hostile Takeover of Childhood*. New York: The New Press.
- Livingstone, Sonia. (2006). Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. In *Computers, Phones, and the Internet: Domesticating Information Technology*. Kraut, R. E., M. Brynin et S. Kiesler., éd. New York: Oxford University Press.
- (2003). Children's Use of the Internet: Reflections on the Emerging Research Agenda. *New Media & Society* 5(2): 147-166.
- Livingstone, Sonia et Magdalena Bober. (2003). *UK Children Go Online: Listening to Young People's Experiences*. Londres : Economic and Social Research Council.
- (2004). *UK Children Go Online: Surveying the Experiences of Young People and their Parents*. Londres : Economic and Social Research Council.
- Montgomery, Kathryn. (1996). *Web of Deception: Threats to Children from Online Marketing*. Washington: Center for Media Education.
- Réseau Éducation-Médias. (2004). *Jeunes Canadiens dans un monde branché : Phase II*

– *Groupes de discussion*. Ottawa.

(2000). *Groupes de discussion de parents et de jeunes, 2000*. Ottawa

Neopets. Astuces sur la sécurité : <http://www.neopets.com/safetytips.phtml>.

Neopets. Politique de protection de la vie privée : <http://www.neopets.com/privacy.phtml>

Seiter, Ellen. (2004). The Internet Playground. In *Toys, Games, and Media*. Jeffrey Goldstein, David Buckingham et Gilles Brougère, édés. Mahwah, NJ: Lawrence Erlbaum Associates.

Shade, Leslie Regan, Nikki Porter et Wendy Sanchez. (2005). « You Can See Anything on the Internet, You Can Do Anything on the Internet! » : Young Canadians Talk About the Internet. *Canadian Journal of Communication* 30(4): 503-526.

Steeves, Valerie. (2006). It's Not Child's Play: The Online Invasion of Children's Privacy. *University of Ottawa Law and Technology Journal = Revue de droit & technologie de l'Université d'Ottawa* 3(1): 169-188.

Stern, Susannah R. (2004). Expressions of Identity Online: Prominent Features and Gender Differences in Adolescents' World Wide Web Home Pages. *Journal of Broadcasting & Electronic Media* 48(2): 218-243.

Tang, Shengming et Xiaoping Dong. (2006). Parents' and Children's Perceptions of Privacy Rights in China. A Cohort Comparison. *Journal of Family Issues* 27(3): 285-300.

Turow, J. (2001). *Privacy Policies on Children's Websites: Do They Play by the Rules?* Philadelphia: Annenberg Public Policy Centre of the University of Pennsylvania.

US Public Interest Research Group and Center for Digital Democracy. (2006, 1^{er} novembre). *Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices*. Document déposé devant la Federal Trade Commission.

Youn, Seounmi. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of*

Notes en bas de page

¹ Neopets existe en 11 langues, y compris l'anglais, l'espagnol, l'allemand, le français, l'italien, le chinois traditionnel, le chinois simplifié, le japonais, le coréen, le hollandais et le portugais.

² Astuces de sécurité de Neopets sur:

<http://www.neopets.com/safetytips.phtml>.

Voir également Politique de confidentialité de Neopets sur:

<http://www.neopets.com/privacy.phtml>.

Neopets souscrit à la COPPA.

³ Voir la page de GetNetWise Loss of Privacy, par exemple, sur:

<http://kids.getnetwise.org/safetyguide/danger/privacy>