CANADIAN JOURNAL OF LAW AND TECHNOLOGY
FORTHCOMING 2005

VIRTUAL PLAYGROUNDS AND BUDDYBOTS: A DATA-MINEFIELD FOR TWEENS

Valerie Steeves[*] and Ian R. Kerr[**]

The online world of tweens – kids between the ages of nine and 14 – is fun, interactive, and cool. It is also a place that is structured by seamless surveillance and the aggressive collection of children's personal information. Whether kids are hanging out with Hilary Duff on Barbie.com, playing with Lifesaver products on Candystand, or chatting with ELLEgirlBuddy about their favorite celebrities, a marketer is listening – and sometimes talking – to them, to measure their likes, dislikes, aspirations, desires, wishes, and propensity to purchase product.

This article examines the online places where tweens play, chat and hang out. We argue that the vision behind these places is defined by commercial imperatives that seek to embed surveillance deeper and deeper into children's playgrounds and social interactions. Online marketers do more than implant branded products into a child's play; they collect the minute details of a child's life so they can build a "relationship" of "trust" between the child and brand. Although marketing to children is not new, a networked environment magnifies the effect on a child's identity because it opens up a child's private online spaces to the eye of the marketer in unprecedented ways. Online marketers accordingly invade the child's privacy in a profound sense, by artificially manipulating the child's social environment and communications in order to facilitate a business agenda.

We start by examining five of the web sites which have been identified by tweens as "favorites"[1]. Each site contains examples of marketing practices which are typical of virtual playgrounds, and which turn kids' online play into a continuous feedback loop for market research.

---

[*] Assistant Professor, Department of Criminology, University of Ottawa (vsteeves@uottawa.ca).
[**] Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa (iankerr@uottawa.ca).
Both authors wish to extend their gratitude to the Social Sciences and Humanities Research Council, to the Canada Research Chair program, to Bell, Canada and to the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of the research project from which this paper derives: *On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society*" (www.anonequity.org).

[1] See K. Montgomery, *teensites.com* (2001) Washington: Center for Media Education; L. Shade, N. Porter & K.S. Santiago, "Everyday Domestic Internet Experiences of Canadian Youth and Children", paper presented at Digital Generations, London (26-29 July 2004); F. Filion, *Kids Take on Media* (2003) Ottawa: Canadian Teachers Federation; and Media Awareness Network, *Young Canadians in a Wired World: The Student's View* (2001) Ottawa.

After looking at the places where tweens play, we turn to one of the places where tweens talk. We examine how the principles of human-computer interaction have been used in an instant messaging environment to create virtual "people" that interact with kids, for all intents and purposes, like a real person. By logging the interactions, these BuddyBot programs are able to "learn" about the child and create the illusion of friendship between it and the child. This perfects the relationship between the child and the brand by introducing a virtual person into the equation, a person who is able to give the child ideas about what clothes to wear, what movies to see, what products to buy.

Finally, we provide a brief overview of American and Canadian legislation dealing with children's online privacy, and assess whether or not current laws have been able to protect children's privacy in the online environment. We also examine the ways in which electronic commerce legislation has addressed the role of virtual agents, and assess how well fair information practices can protect kids from the invasive nature of child-bot relationships.

I. VIRTUAL PLAYGROUNDS – THE WORLD OF NEOPETS, TICKLE, CANDYSTAND AND BARBIE

Although adults typically want children to use the Internet because they believe it will give them a leg up at school and prepare them for the workplace[2], kids overwhelmingly prefer to play and socialize online. And the places where they go to play are almost always commercial sites[3].

The corporations that build these sites are interested in kids because of their spending power. It's estimated that Canadian tweens spend $1.7 billion each year of their own money, and influence approximately 12 times that amount if family spending[4]. Corporations that want a share of this market try to attract young traffic by creating web sites that offer online games, quizzes, chat environments and advice. Psychologist Susan Linn[5] argues that these sites are designed to capitalize on children's developmental vulnerabilities; children's need for independence and their desire to communicate with their peers, try on new identities, and express themselves make them more likely to voluntarily provide the site with personal information, so the sites give them plenty of chances to do so.

---

[2] Media Awareness Network, *Canada's Children in a Wired World: The Parent's View* (2001) Ottawa.

[3] *Supra*, note 1.

[4] *YTV Tween Report, Wave 8* (2002) <http://www.corusmedia.com/ytv/research/index.asp#TWEEN>.

[5] Susan Linn, *Consuming Kids: The Hostile Takeover of Childhood* (2004) New York: The New Press.

For example, Neopets is a popular site with the tween set, especially tween girls. The public nature of the Net means that the marketers that operate the site can watch these kids as they play, and record their interests, preferences, communications and behaviour. But to maximize the value of the information they collect, Neopets, like other virtual playgrounds, encourages the kids to identify themselves. If a child playing on the site tries to access a game or a contest, he or she is told, "OOPS! YOU ARE NOT LOGGED IN! You are not currently logged into Neopets, so you will NOT be able to earn any Neopoints for playing this game (but it'll still be fun!) Either Log In, or Sign Up with Neopets and you can start earning Neopoints straight away!" The site tells kids registering is "simple, fast and FREE!", although the sign-up process involves accepting Terms and Conditions that are 18 screens long, and the default setting on the sign-up form commits them to installing software like "GloPhone, so I can call anyone, anywhere for Free (GloPhone to GloPhone) right from my computer. Get 500 NP [Neopoints] for signing up!"

Once a child registers and provides the site with her first and last name, email address, date of birth, gender, city, state/province, country and zip/postal code, she can create a virtual pet to play with. Although there are "soup kitchens" for "poor" Neopets, the children who play in the Neopet "community" are encouraged to earn Neopoints to pay for food and toys for their pets. In fact, the site warns kids not to create too many pets, "as very soon they will begin to get very demanding."[6]

To keep their Neopets happy, kids earn Neopoints by filling in market surveys that ask detailed questions about their preferences. For example, one survey in 2002 focused on food, and asked kids about their:

- favourite chocolate bars and cereal brands;
- breakfast habits;
- education level;
- ethnic background; and
- Internet use.

It also asked children to select things that interested them from a list of 60 items, including gambling, cigars, beer and liquor[7].

Although kids willingly provide this information in order to play in the Neopets community, there is little on the Neopets site that indicates their playground is actually a commercial space. Marketing pitches are soft, and couched in terms of their interest to kids. For example, when kids

---

[6] Neopets create.a.pet page < http://www.neopets.com/addpet.phtml>.

[7] Valerie Steeves & Jane Tallim, *Kids for Sale: Online Marketing to Kids and Privacy Issues* (2004) Ottawa: Media Awareness Network.

register with the site, they are encouraged to sign up for Return Path: "Who might be looking for you at your old e-mail address? Stay in touch with friends at your current e-mail. Enter your old e-mail address to register for Return Path's free service. Get 250 NP for signing up!"[8] But Return Path's service is actually intended to benefit email marketers. When kids provide their old and new email addresses, they are passed onto marketers to help them "[navigate] the ever-changing email landscape. Our solutions protect brands, increase efficiency, and improve results... Return Path helps you [the email marketer] increase ROI [return on investment] by continually improving your email communications"[9].

Tickle.com uses similar tactics to get older kids to divulge personal information so it can be used to target them with personalized advertising. For example, when 14-year-old Jenna took the "Ultimate Personality Test" on Tickle's predecessor, Emode.com, she was told, "you value your image," so Emode recommended that she visit e-diets, one of their advertisers, to "prep her bod for success"[10]. Although many corporations, like Tickle, use stereotypes to reinforce social messages about body image and gender roles,[11] the effect of these stereotypes is "magnified in a surveillance environment that enables marketers to embed them in a personalized communications with an individual child"[12].

In addition, since kids have to register to fill out any of the many quizzes on Tickle, the quiz results are matched to the child's first and last name, gender, date of birth, zip code/postal code, education, and "relationship status"[13], in effect creating a detailed marketing dossier on each kid that registers on the site. However, the site's privacy policy paints a different picture. It reads:

> Tickle is an online media company that brings you fun, insightful, and personalized information in our emails and on our website. We want to give you information that you care about and that is relevant to you. So, we enter into a voluntary relationship with you where we listen to who you are, and what you want. Then we go out and find it and bring it back to you in the most personalized services possible. It's that simple, and it's that cool

---

[8] Neopets sign.up.now page <http://www.neopets.com/signup/signup.phtml?agegroup=3>.

[9] *Ibid*.

[10] Steeves & Tallim, *supra*, note 7.

[11] N. Signorelli, *A Content Analysis: Reflections of Girls in the Media* (1997) Menlo Park, California: Kaiser Family Foundation/Children Now.

[12] Steeves & Tallim, *supra*, note 7.

[13] <http://web.tickle.com >.

> — our emails and services are all about you and the data you disclose to us makes it possible to deliver what you truly want[14].

In contrast to Tickle, the commercial nature of kids' online playgrounds is more readily apparent on branded game sites because on these sites, the product is embedded into the site itself. Candystand is a popular site among boys and girls between the ages of nine and 17. Candystand is owned by Kraft and every game on the site features Lifesavers products. For example, "Boardwalk Bowling" is played by rolling a virtual ball into a group of Lifesaver candies for points. By building brands into play environments, marketers create what they call "sticky traffic"; although kids won't stare at an ad for hours, they'll play with an online brand until their parents turn off the computer.

Like other kids sites, Candystand encourages kids to register, so their online actions can be matched with their personal identities. But Candystand also embeds games with adult content into its site. For example, in "Video Poker", kids bet credits on poker hands that appear in a slot machine. When they win, they hear the sound of coins clinking as the number of credits increases. In "Poker Puzzler", cards are dealt onto a casino table amid lounge music and background conversation. When kids win this game, they're rewarded with slot machine sounds.

Playgrounds that create product loyalty for adult products are not uncommon on the Net. Beer.com is another popular site among tween and teenaged boys[15]. Like Candystand, Beer.com tells boys to, "Join now and get access to the best on the Web for free! The Pub Club is where we keep Beer.com's premium content. You'll find beer.com's famous Beer Girls, contests, incredible features, the best beer ads and other awesome vids. And when we create something unbelievably cool, you'll find it in the Pub Club." Encouragements to join up are embedded in the site. For example, visitors are advised to, "Log-in to see two girls kissing and a bunch of other kickass beer ads." To register, users provide their name, email address, age, gender, country, and zip/postal code, and answer the question, "How many beers do you drink per week?" by selecting 0, 1 to 2, 3 to 6, 7 to 12, or 13+. If teens under 18 try to register, they are advised that, "You must be of legal drinking age to join." However, simply changing the birth date on the registration form allows them to complete the registration process, even though they have already identified themselves as underage users.

---

[14] < http://web.tickle.com/about/privacy.jsp>.

[15] Media Awareness Network, *supra*, note 1.

Although branded playgrounds collect children's personal information, their main purpose in doing so is to create a relationship between the brand and the child[16]. Like Candystand, Barbie.com offers plenty of opportunities for girls to interact with the Barbie brand[17]. Girls can design and dress their own Barbies, do a Barbie make-over, sing along with Barbie as she sings "Friends like we are" to the child, or "Make Happy Family Memories" with the Barbie's "friends" Alan, Midge, their son Ryan, Midge's parents, and Midge's new baby (who the child gets to name when she fills out the Birth Certificate).

The site actively encourages girls to buy Barbie products. For example, each child can record their purchasing preferences in their "Wish list", and email it to their parents. But the site incorporates more than a sales pitch – it reinforces the "friendship" between the child and the brand itself. After taking a car trip into the city to help Cali (a doll) get ready for a party, the screen tells her, "We're totally glad you're chillin' with our Cali girl crew!" For $1.99 (US), Barbie can also call the child directly on the phone. The site tells girls, "Wow! You could get a call from your best friend – Barbie!" For 2004 American Thanksgiving, Barbie told the girls in audio, "Hi! It's Barbie! I think this is such a special time of year. Don't you? I've got a wonderful wish for you. I'd love to call you and tell you! Or just say Hello. Ask your mom or dad if it's okay. Oh, I hope to talk to you soon!" Barbie will also call to wish them Happy Birthday, invite their friends to a party at their house, or tell them a bedtime story.

Through interacting with a product in a web environment, children learn to "trust" brands like Barbie and consider them their "friends"[18]. That "friendship" becomes even more palpable with the use of virtual sales representatives, or BuddyBots.

II. BUDDYBOTS[19]

---

[16] M. Lindstrom & P.B. Seybold, "UK school plans retinal scan in the dinner queue" (2003) *The Register*.

[17] Younger tweens continue to report Barbie as a favourite site: Media Awareness Network, *supra*, note 1.

[18] Media Awareness Network, *supra*, note 1; Media Awareness Network, *Young Canadians in a Wired World: Phase II Focus Groups* (2003) Ottawa.

[19] Many elements from this section are excerpted from Ian R. Kerr, "Bots, Babes and the Californication of Commerce" (2004) 1 *University of Ottawa Law and Technology Journal* 285-323. The term "BuddyBots" was coined by Marcus Bornfreund in Ian R.Kerr and Marcus Bornfreund, "BuddyBots: How Turing's Fast Friends are Under-Mining Consumer Privacy" (forthcoming, 2005) *Presence: Teleoperators and Vistual Environments.* Many elements from this section are excerpted from Ian R. Kerr, "Bots, Babes and the Californication of Commerce" (2004) 1 *University of Ottawa Law and Technology Journal* 285-323.

Having looked at the virtual playgrounds where tweens play online, let's visit one of the places where they talk. MSN Instant Messaging is now one of the primary methods of communication used by Canadian tweens and teens[20]. Instant messaging space is automated, a world equally at home to people and bots. The commercial interlocutors who populate this space have been built, not born. The vision underlying the architecture of this place is, as we have seen, inspired by commerce and its migration deeper and deeper into electronic environments. In this strange place, few of the interactions are carried out *exclusively* by human beings. Intelligent software agents are employed to assist tweens with many time-consuming activities. By *automating* shopping, surfing and searching – and even talking – young consumers and merchants are said to be able to reduce transaction costs and free-up time. To make these online interactions even more automated, more appealing and more trustworthy, programmers in the field of "Human-computer interaction" (HCI) are applying various principles of psychology in the development of a number of interesting and, in some instances, troublesome applications for electronic commerce.

One such application is a bot named Nicole.[21] Nicole is an automated virtual representative[22], used in e-business for customer service, sales and marketing. Nicole answers questions in real time and uses natural language. Here is an example of a spontaneous conversation that Ian once had with her. (His own thoughts during the conversation are represented in italics):[23]

> Nicole: Hi my name is Nicole. I am a virtual representative. Please tell me your name.
> Ian: My name is Ian.

---

[20] Media Awareness Network (2003), *supra*, note 1.

[21] More specifically, Nicole was a vRep available at NativeMinds, <http:/www.nativeminds.com>. NativeMinds was recently acquired by Verity, <http:/www.verity.com>. Verity still markets vReps under the product category "Verity Response," <http:/www.verity.com/products/response/features.html>. Vreps operate on the basis of "pattern matching" and build on a variety of artificial intelligence techniques that have evolved since the time that Alan Turing first created the challenge of inventing a machine that could imitate human conversation well enough to fool a human being into thinking that's/he was interacting with another human being. The original "Turing Test", as it is now famously known, is set out in A.M. Turing, "Computing Machinery and Intelligence" (1950) *Mind 49:* 433-460.

[22] "vReps are virtual representatives…used to humanize online relationships by providing a single, interactive contact point for all customer questions through a natural language dialog...[vReps] intelligently answer each user's question based on their needs and [a company's]…business objectives": see NativeMinds, "About Us", <http:/nativeminds.com/AboutUs_default.html> Some examples of vReps used by major companies include "Katie" (a vRep that offers skincare information to *Dove* customers); "Hank" (who provides information on employment opportunities at *Coca Cola*); and "Anne" (who offers nutritional information and *Iams* product recommendations to pet owners): see "Customers," <http://nativeminds.com/Customers_default.html>. These links now direct you to the website of Verity, which recently acquired NativeMinds, and markets vReps under the product category "Verity Response."

[23] Of course, Ian makes no representations as to what Nicole might or might not have been thinking about at the time. ;)

> Nicole: Hi Ian! What would you like to know about NativeMinds, the leading provider of vRep solutions?
> Ian: Tell me […] about your vReps.
> Nicole: vReps are Web-based programs that provide 24 x 7 customer service by conversing with customers in real-time, natural language and answering questions about companies' products and services.
> Nicole: Are you ready to ask some more questions?
> Ian: Are vReps legal?

Here, Ian purposely asked a vague question to see how Nicole would handle it.

> Nicole: If you have any questions regarding anything that might involve our legal department, try asking me a specific question or email us at info@nativeminds.com

At this point Ian was practically ready to admit that Nicole was demonstrating signs of intelligence and perhaps even the possibility that she spent three years in law school—the skill she demonstrated at evading questions was on par with that of Ian's very best students. Consequently, Ian decided to ask a more precise legal question to really test her.

> Ian: What are your licensing arrangements?
> Nicole: Generally, we license our software based on the number of concurrent conversations a vRep will have. However, we do offer other licensing structures such as enterprise licenses, which handle an unlimited number of simultaneous conversations.

Ian had an inkling, at this point, that Nicole might simply be responding to keywords… so Ian decided to throw her a bit of a curveball.

> Ian: Wow, you are totally cool!
> Nicole: I'm glad that you approve! Whenever you are ready, I'd be happy to tell you more about Native Minds and its products.

Feeling pushed around by a bot, Ian responded in kind.

> Ian: But I don't really have any more questions!!
> Nicole: Come on, you have got to have more questions.

Her quick comeback annoyed Ian and put him on the offensive.

> Ian: Okay smartie-pants—do you even remember what I asked you before?
> Nicole: I can remember things about you and things you say, where I have been programmed to. For example, Ian, you recently said: "what are your licensing arrangements?"
> Ian: How do vReps think so fast?

> Nicole: vReps like me operate by *pattern matching*. A vRep compares a user's questions with possible answers and selects the answer most appropriate for the questions asked.

Ian decided that it was time to get philosophical with Nicole.

> Ian: But that is not truly "thinking," or is it?
> Nicole: Another user told me that Thinking was just neurons firing in random directions, surely the same can be done with circuits.

At this point Ian thought Nicole (more likely, her programmers) to be clever. But, upon reflection, he realized that the reductionist representation of Thinking that was offered cannot adequately capture the notion of "moral thinking," a notion that will require greater understanding and application as more and more entrepreneurs become interested in machine thinking and its possible applications in electronic commerce.

Another example of an HCI application is ELLEgirlBuddy,[24] the vRep for teen magazine ELLEgirl. Living in San Francisco with her parents and her older brother, ELLEgirlBuddy represents herself as a redheaded sixteen-year-old who likes kickboxing and French class. Her favorite color is periwinkle. 'Catcher in the Rye' is her favorite book. She watches 'Buffy the Vampire Slayer' and listens to 'No Doubt.' When she grows up, she wants to design handbags, own a bookstore café and work overseas as a foreign correspondent. With the aim of steering internet traffic towards the ELLEgirl.com web site, ELLEgirlBuddy is programmed to answers to questions about her virtual persona's family, school life and her future aspirations, occasionally throwing in a suggestion or two about reading ELLEgirl magazine. Writing sometimes about her own professed body image problems, ELLEgirlBuddy presents herself as someone whom other teenagers might confide in. And they have done so by the millions.[25] Here is a sample of her jive and jingle:

> "i looove making my own clothes," ELLEgirlBuddy says in an instant message. "i use gap tees a lot. you just shrink em and add ribbons. insta-chic! i like kick-boxing (major crush on gabe, my kickboxing instructor! :-*). reading... i like 2 curl up with a book and an extra-chocolaty mocha. yum! u?"[26]

---

[24] Who used to live at <http://www.ellegirl.com/activebuddy/index.asp> but has subsequently been "retired".

[25] ELLEgirlBuddy has subsequently been retired: <http://www.activebuddy.com/agents/retiredagents.shtml>/

[26] Christine Frey, "Web friend or faux?" *Los Angeles Times* (18 July 2002). See also Bob Woods, "Case Study: ActiveBuddy/ELLEgirlMagazine" *InstantMessagingPlanet* (26 June 2002), <http://www.instantmessagingplanet.com/public/article.php/10817_1375971>.

In just a few short years, ELLEgirlBuddy and other bots, such as SmarterChild, have chatted with millions upon millions of people. In part, their popularity stems from the fact that their conversations are not only interesting and engaging but *voluntary*.[27] To their credit, the creators of these bots recognized the extreme distaste that consumers have for push-based marketing strategies. As ActiveBuddy's C.E.O. Steve Klein recently put it, "[t]he last thing we want to do is wreck this medium by pushing marketing communications to users that they don't want, as has happened in email marketing with SPAM."[28] In contrast to SPAM advertising, SmarterChild and ELLEgirlBuddy do not thrust messages upon consumers against their will. Instead, they claim to use "a fully *opt-in*, *pull* model that *invites* users, in effect, to obtain branded content via IM."[29]

Effective marketing depends on the ability of the person pushing a message to establish trust.[30] The goal of ActiveBuddy agents such as ELLEgirlBuddy was to enhance their language-parsing and response capabilities so that "these agents will become, for all intents and purposes, actual *friends* of the people that interact with them…[such that] the agents' recommendations will be taken as being on a par with, for instance, your recommendation to me that I buy a Volvo."[31] A possible motto for this fascinating business model: *virtual trust through virtual friendship.*

ActiveBuddy Inc. and other such companies are attempting to *create the illusion of friendship* by developing "user logs that enable the agents to gather and retrieve information about users, so that they can understand a user's emotions, schedules, and so on."[32] In other words, these companies are constantly collecting incoming data from users and storing that information for the purposes of future interactions.[33] Most people who regularly exchange instant messages with their digital buddies would have no idea that enormous personal profiles are being constructed about them,

---

[27] Though, as it suggest below, it is not *truly* voluntary as it is not founded on informed consent.

[28] Interview of Steve Klein, CEO of ActiveBuddy Inc. [n.d.] "ActiveBuddy & IM Advertising: A Quiet Revolution", <http://www.avantmarketer.com/stevekleinprint.htm> ["Quiet Revolution"].

[29] *Ibid*. [emphasis in original].

[30] Frederick F. Reichheld & Phil Schefter, "E-Loyalty: Your Secret Weapon on the Web" (2000) 78 Harv. Bus. Rev. 105; Sirkka L. Jarvenpaa & Emerson H. Tiller, "Customer Trust in Virtual Environments: A Managerial Perspective" (2001) 81 B.U.L. Rev. 665; G.L. Urban, F. Sultan & W.J. Qualls, "Placing Trust at the Center of Your Internet Strategy" (2000) 42 Sloan Mgt. Rev. 39.

[31] "Quiet Revolution," *supra* note 28.

[32] *Ibid.* Of course, such claims are not so boldly stated in the company's privacy policy.

[33] And perhaps for other purposes.

or about the fact that these profiles are being used to affect (as well as effect) their subsequent interactions.

The cycle that recurs here could turn vicious—by mining massive amounts of unprecedented user data derived from spontaneous, trusted, one-on-one conversation, bots will become better and better at imitating friendship. And the better that bots get at imitating friendship behavior, the more personal information they will be able to cull from their conversations. When one combines this recurring cycle with rapid advances in AI and HCI, the *virtual friendship* business model not only opens up entirely new realms of targeting potentials for advertisers, but also for more sinister forms of surveillance as well.

III. VIRTUAL PLAYGROUNDS, BUDDYBOTS AND THE LAW

Invasive marketing practices and the commodification of children's social spaces have generated public debate for the past four decades[34]. After the dangers of online marketing practices were first revealed in 1996 with the publication of the Center for Media Education's report, *Web of Deception*[35], the US Congress passed the *Children's Online Privacy Protection Act of 1998*[36] (COPPA).

Under COPPA, operators of commercial web sites directed to children that collect personal information from children under the age of 13 must comply with a set of fair information principles. First and foremost, operators are required to obtain parental consent before collecting information from a child. The parent's consent must be "verifiable" – in other words, the operator must take reasonable steps to ensure that the parent receives notice of the operator's information practices and consents to them. The FTC informs operators that "if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required". Internal purposes include "marketing back to a child based on his or her preferences or communicating promotional updates about site content" (US, 2004b). Accordingly, the law assumes that placing children under surveillance as they play, and collecting their

---

[34] As Linn notes, debate around online marketing is contextualized by the broader movement to regulate children's advertising as a whole. This movement began in the 1960s and continues today (Linn, *supra,* note 5, at p. 200).

[35] K. Montgomery, *Web of Deception: Threats to Children From Online Marketing* (1996) Washington: Center for Media Education.

[36] 15 U.S.C. §§ 6501-6506.

personal information in order to market product to them, is inherently benign and poses only a slight risk of harm.

Canadian legislators have not dealt specifically with children's privacy and the *Personal Information Protection and Electronic Documents Act*[37] is silent with respect to children. However, the Office of the Privacy Commissioner's *Guide for Businesses and Organizations* indicates that consent for a minor may be obtained from a legal guardian[38]. Since, under the common law, a minor has a diminished capacity to enter into a contract, it is likely that a court would hold that a person under the age of 18 in Canada cannot legally consent to disclose his or her personal information for the purposes of PIPEDA without parental consent.

Both of these Acts assume that the presence of online privacy policies will enable parents and older children to make informed decisions about whether or not to release personal information. However, this assumption is problematic. First, it assumes that parents (and children 13 and over in the US) actually read and understand online privacy policies. Turow[39] reports that 57 per cent of adults incorrectly believe that the mere presence of an online privacy policy ensures that any personal information that the site collects will not be shared with other organizations. Although 47 per cent say they think privacy policies are easy to understand, two-thirds of the people who believe this also – incorrectly – believe a site will not share their data. Most children, on the other hand, are unlikely to read a privacy policy because they are long and boring[40] and they simply consent to provide the information because they want to enter a contest or win a prize[41].

In addition, distinguishing children based on age, like COPPA does, arbitrarily divides teenagers and younger children. Allen argues that, "No justification exists for perceiving the age of 13 as more capable of using computers without adult supervision. Some children above the age of 13 may still need parental control and vice versa"[42]. From a child's point of view, the age limit is incredibly easy to sidestep. If a 12 year old really wants to collect those Neopoints, play a game on Candystand, or chat on

---

[37] S.C. 2000, c. 5.

[38] Privacy Commissioner of Canada, *Your Privacy Responsibilities: A Guide for Businesses and Organizations* (2004) Ottawa: Public Works and Government Services Canada.

[39] J. Turow, *Americans and Privacy: The System is Broken* (2003) Philadelphia: Annenberg Public Policy Center of the University of Pennsylvania.

[40] Media Awareness Network (2003), *supra*, note 1.

[41] Media Awareness Network (2003), *supra*, note 1.

[42] Quoted in Electronic Privacy Information Center, *The Children's Online Privacy Protection Act* (2003), <http://www.epic.org/privacy/kids>.

beer.com, all she has to do is change her age. On Candystand, for example, a child who registers an age less than 13 is asked for a parent's email address so the site can ask for the parent's permission to register the child. But if the child simply goes back to the registration page and changes her age, she is registered automatically. Unless every user's age can be authenticated, age limitations are virtually unenforceable, but reliable authentication would paradoxically lead to a massive invasion of online privacy forcing every user to identify himself to prove that he is not a child[43].

Perhaps most telling is the fact that, from a practical point of view, both Acts have failed to slow the sale of children's personal information. EPIC concludes that, "Despite COPPA's protections, there is a thriving list brokerage industry that targets children" and points to a "pre-school list advertisement, where marketers can purchase one million names for only $5"[44]. Shade, Porter and Santiago conclude that, "Internet policy has so far tended to ignore how children and teens have become a viable and integral online market, which is a startling omission when considering the overall political economic framework of the Internet"[45].

Accordingly, measures mandating consent and transparency have been ineffective in protecting kids' online privacy.

There are also problems with the legal framework dealing with BuddyBots. AI and HCI research has come a long way during the past few years. Although primitive, vReps and other bots already *behave* in ways that alter the rights and obligations of the people with whom they interact. Bots now have the ability to create rights and obligations. In most provincial electronic commerce legislation in Canada, the deeming provision takes the form of some kind of permission. For example, the Uniform Electronic Commerce Act stipulates that:

> A contract may be formed by the interaction of an electronic agent and a natural person or by the interaction of electronic agents.[46]

What has gone practically unnoticed, however, is the fact that by exploiting basic HCI techniques, not to mention affective computing research, bots can be used in electronic commerce to make representations

---

[43] Electronic Privacy Information Center, *ibid*.

[44] *Ibid.*

[45] Shade et. al., *supra*, note 1.

[46] Several provinces have adopted this section. See *e.g. British Columbia*, *supra* note 10, s. 12; *Ontario*, *supra* note 10, s. 20; *Nova Scotia*, *supra* note 10, s. 22; *Prince Edward Island*, *supra* note 10, s. 20; *Saskatchewan*, *supra* note 10, s. 19.2.

that seem believable and trustworthy to the consumers who interact with them in online commerce. What has also gone unnoticed is that some potential uses of HCI applications could become problematic from a legal perspective. And these potential problems are not currently addressed in existing electronic commerce legislation.

The *Canadian Code of Practice for Consumer Protection in Electronic Commerce* was developed "to establish benchmarks for good business practices for merchants conducting commercial activities with consumers online."[47] Having recently undergone pilot testing by a number of industry sectors, the *Canadian Code* is currently under review.[48] The reviewed and revised version of the *Canadian Code* will be available for endorsement by all interested and will ultimately be published. Whether it will ever carry the force of law remains unknown.

When considering whether it is necessary to clarify the law so that it better protects consumers participating in automated environments, a number of the core principles found in the *Canadian Code* are worth keeping in mind. The three principles most relevant to our examination of automated electronic commerce are set out and briefly discussed below. The first relevant principle has to do with the manner in which information is provided to consumers. According to the *Canadian Code*:

> 1.1 Vendors shall provide consumers with sufficient information to make an informed choice about whether and how to complete a transaction. All of the information requirements described in this code must be:
> a) clearly presented in plain language;
> b) truthful;
> ...
> 1.2 Vendors shall ensure that their marketing practices…are…not deceptive or misleading to consumers…
> ...
> 3.1 Vendors shall take reasonable steps to ensure that consumers' agreement to contract is fully informed and intentional.[49]

As illustrated in the preceding section, many consumers who transact with Nicole, ELLEgirlBuddy and the like will not fully appreciate the nature of their transactions. Arguably, the marketing practices associated with some of these automated services are misleading, perhaps even deceptive. While

---

[47] *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (Approved in Principle January 2003), <http://strategis.ic.gc.ca/pics/ca/eng_consumerprotection03.txt> [*Canadian Code*].

[48] By a body known as the *E-Commerce Leaders Code Review Committee*. See <http://strategis.ic.gc.ca/pics/ca/eng_consumerprotection03.txt>.

[49] Canadian Code, *supra* note 47.

there are many tech-savvy consumers, information provision in some automated environments can constrain the possibility of informed decision-making for the vast majority of consumers. The second relevant consumer protection principle articulated in the *Canadian Code* concerns online privacy:

> 4.1 Vendors shall adhere to the principles set out in Appendix 2 with respect to the personal information they collect from consumers as a result of electronic commerce activities.[50]

By exploiting HCI and affective computing techniques, marketers such as ActiveBuddy Inc. have made it possible to surreptitiously *yet openly* collect sensitive but extremely valuable personal information – under the guise of a so-called voluntary "fully *opt-in, pull model*."[51] Although their claim would be that consumers freely choose to chat with ActiveBuddy bots and that the consumers decide for themselves what they want to say and not to say, such claims are unconvincing in light of the basic structure of their business plan.

The fair information practices set out in Appendix 2 of the *Canadian Code*[52] contain a number of requirements that are clearly not respected by ActiveBuddy and many other bot-based business models. For example, Principle 2 stipulates that "[t]he purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."[53] The closest ActiveBuddy comes to offering an identifying purpose for the information that it collects is "in order to enhance your experience."[54] Given that the actual reason for logging all personal conversations is so that ELLEgirlBuddy is able to trick children and other consumers into thinking that they are chatting with actual friends, the identifying purpose as stated in the corporate privacy policy is disingenuous at best.

Without properly identifying the purposes of information collection, many automated services circumvent the third principle of the *Canadian Code*—arguably the cornerstone of fair information practices—which states that the "knowledge and consent of the individual are required for the collection, use, or disclosure of personal information…".[55] Identifying

---

[50] *Ibid*.

[51] "Quiet Revolution", *supra* note 28 [emphasis in original].

[52] These form the basis of the *Model Code for the Protection of Personal Information* (CAN/CSA - Q830-96; published March 1996; reaffirmed 2001), <http://www.csa.ca/standards/privacy/code/>.

[53] *Ibid*.

[54] ActiveBuddy privacy policy < https://www.buddyscript.com/privacy.html>; SmarterChild privacy policy <http://www.smarterchild.com/privacy.shtml>.

purposes aside, most consumers have no idea that their conversations are logged and, if they knew, they *would not* consent to them being logged.

The fourth and fifth principles of fair information practices are also jeopardized. They require that the "collection of personal information shall be limited to that which is necessary for the purposes identified by the organization"[56] and that "[p]ersonal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law."[57] Recall that, in order to "enhance experience," vReps and digital buddies log every single interaction.

In addition to information provision and online privacy, there is a third consumer protection principle articulated in the *Canadian Code* that is relevant. This provision concerns online communications with children:

> 8.1 Online activities directed at children impose a social responsibility on vendors. All communications to children, or likely to be of particular interest to children, 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 a product.
> ...
> 8.3 Vendors shall not collect or disclose children's personal information without the express, verifiable consent of their parents or guardians… When seeking parental consent, vendors shall clearly specify the nature of the proposed communications, the personal information being collected and all potential uses of the information.
> ...
> 8.4 Vendors shall not knowingly send marketing email to children.[58]

Digital buddies such as ELLEgirlBuddy, though they may not intentionally target persons who have not reached their thirteenth birthday,[59] certainly do communicate with children and/or are of particular interest to children. By offering up anecdotes about her own family, body and personal life experiences in exchange for any personal information offered up by the young consumer, ELLEgirlBuddy might plausibly be

---

[55] *Canadian Code*, *supra* note 47, Appendix 2, principle 3.

[56] *Canadian Code*, *supra* note 47, Appendix 2, principle 4. Principle 4 also requires that information shall be collected by fair and lawful means.

[57] *Ibid*., Appendix 2, principle 5. Principle 5 also states that "[p]ersonal information shall be retained only as long as necessary for the fulfillment of those purposes."

[58] Canadian Code, *supra* note 47.

[59] Which is the defined age of childhood according the *Canadian Code*. Arguably, they do target such persons.

said to "exploit the credulity, lack of experience or sense of loyalty of children." ActiveBuddy would likely respond to such claims by pointing out, once again, that all buddy-based communications are consensual since all topics of discussion are *always* initiated by the consumer, not the bot. Consequently digital buddy-child interactions would not violate principle 8.4.

Regardless of whether Nicole or ELLEgirlBuddy can actually be said to violate existing consumer protection principles found in the *Canadian Code* or elsewhere, there is a clear need for further study of consumer protection in the context of automated electronic commerce—especially in the context of protecting tweens.

IV. CONCLUSION

In this article we have investigated the online spaces that children between the ages of 9 and fourteen inhabit. The architecture of these spaces, we suggest, fosters and facilitates intensive corporate surveillance. Hardly child's play, these spaces and the machine-based creatures that inhabit them are an easy and inexpensive means of "exploit[ing] the credulity, lack of experience or sense of loyalty of children." They are also an illicit means of gathering personal information about millions if not billions of other people in clear violation of the principles of *fair information practices* that have been adopted in one form or other around the globe.

For the most part, these practices and their broad social implications have gone unnoticed. Are we in need of special rules to govern the safety of children in virtual playgrounds? Should our consumer protection principles specifically address issues that arise when Barbie and other avatars are used *instead of people* as the primary source of interaction and information exchange? Should the law treat BuddyBots and other vReps the same as people during the negotiation and formation of a contract? Are there *any* human functions that we ought to prohibit machines from carrying out in this or other contexts? The aim of this article is, in part, to raise questions such as these and to promote further research and writing on this much neglected subject.