Gaming privacy: a Canadian case study of a co-created privacy literacy game for children

Surveillance & Society

Article

Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children

Kate Raynes-Goldie

Curtin University, Australia.
k.raynes-goldie@curtin.edu.au

Matthew Allen

Deakin University, Australia.
matthew.allen@deakin.edu.au

Abstract

This paper reports the process and outcomes of the design process of a game which educates children about management of privacy online. Using a participatory action research process informed by ethnographic data collection, children worked with the researchers to develop and play a game which simulates certain aspects of online privacy management as well as creating scaffolded experiential learning in a safe environment. The game allows children to develop autonomous skills and understandings, not only for more effective learning but also because it is only through autonomy that children can develop a sense of self which is necessary for understanding what it means to be private. The paper shows that children have quite sophisticated understandings of privacy, compared with some adult perceptions, and that these understandings include awareness of the risks posed by commercial organisations seeking to gather personal data from them. More broadly, the paper suggests that the engagement of children as research and design participants can lead to more successful approaches in the development of privacy literacy.

1. Introduction

The increasing use of the internet and social media in everyday life has seen growing concern about online safety and privacy, particularly with respect to children. Such concern is primarily expressed by adults and, accordingly, most initiatives are based on adult perceptions of children's technology uses. The resulting initiatives, in the form of government legislation, educational programs, or parental control applications do not account for the experience and needs of children, nor their status as social actors. Sometimes, these approaches can do more harm than good (Marx and Steeves 2010; Nolan, Raynes-Goldie and McBride 2011). Importantly, these initiatives do not foster the development of children's autonomous understanding of privacy (see Nolan, Raynes-Goldie and McBride 2011: 25-26). Based on this difficulty, we hypothesised that by engaging children with online privacy in a way that both respected and encouraged their autonomy as well as their status as social actors, they would be better able to develop their privacy literacy skills and thus be better equipped to make appropriate privacy decisions. Further, these privacy literacy skills need to be learned, not taught, and emphasise the risks and concerns that children themselves were expressing, rather than those imagined by adults. To this end, we undertook a two stage participatory action research project involving the design of a privacy literacy game with children as co-participants in the both the research and the design process. In the first stage, using collaborative facilitation techniques and ethnographic data collection, the researchers worked with the children to determine their current understandings of privacy with a particular focus on what they knew and what they wanted to know more about. This information was key to establishing the content and focus

Raynes-Goldie, K. and M. Allen. 2014. Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children. *Surveillance & Society* 12(3): 414-426.
http://www.surveillance-and-society.org | ISSN: 1477-7487

of the second stage, which was the actual game co-creation. This paper details the foundations, processes and results of the project, titled *Gaming Privacy*, including both an overview of what the young co-creators already knew about privacy and the game's effectiveness in facilitating the autonomous decision making skills that are, ultimately, the most effective way for children to be both safe and in control online.

2. Social media, children and privacy

For many people, daily life involves regular, often extensive, use of internet media and communications tools for human interactions in a shared digital environment. Such social media participation has become an everyday occurrence that no longer stands separate from other, non-networked activities (as explored comprehensively in Rainie and Wellman 2012). Many uses of the internet today, and social media in particular, depend on, or readily lead to, disclosure of people's 'actual' identities, situating them in known contexts and leaving limited separation between digital and physical presentations and performances of self (Dwyer et al. 2007; Tufekci 2008; and Debatin et al. 2009). Unlike early forms of online communication, largely driven by the possibility of a separation between online and offline selves, now there are simply different modalities of a single self.

There is no one cause of these changes in the way humans share themselves via the internet. Commercial exploitation, more ubiquitous connectivity and mobile devices, and the emergence of Facebook as a dominant online interaction form, have all played their part. One significant consequence has been an increasing realisation that the internet, far from offering a private space in which to conduct social relations, is now a place where we might find ourselves more exposed, and perhaps more at risk. We now live in a time of socially mediated publicness, in which 'social mediation blurs boundaries and pushes mutual redefinition between public and private' (Baym and boyd 2012: 322). Users of social media always now negotiate the extent to which they are releasing information which might normatively be considered private (that is, whose release beyond a very specific set of trusted personal relationships might damage the individual concerned). Yet this negotiation can be unrealised, or worse, simply demanded, assumed or occur covertly (Schrammel et al. 2009: 276). Social media participation often does not provide cues that might remind people to be conscious of their privacy; moreover the digital environments that appear private can often become, without any significant effort or forewarning, entirely too public.

A related consequence of the rise of social media is that young people are consistently positioned in public debates as both *more* capable and yet also *more* incapable than older people (especially those who remember the transition to a networked world). It is regularly assumed that young people have high levels of technical skill in engaging with digital network media but lack equal skill in judging how to act online. This assumption of the inherent vulnerability of younger members of society is, of course, common to many activities. However, the higher level of skill in digital media is construed as exacerbating, not militating against, this lack of judgement, for younger people have ready access to modes of interaction and social engagement which they do not (it is claimed) yet know how best to manage. The most extreme form of this concern is that even when control is imposed, in some technological form, young people may 'possess skills and social practices [that] can effectively undermine the effectiveness of technical solutions to protect them from online risks' (Bryce and Klang 2009: 160).

A regular focus of both news reporting and scholarly research into the internet is the threats, potential and actual, which young people might encounter online, stemming from this status as naïve experts in an environment where privacy management is more complicated and yet very necessary (Livingstone 2006; Tufekci 2008; Raynes-Goldie 2011). The threat most regularly identified is that of sexual predation (Barnes 2006; boyd and Jenkins 2006; Albrechtslund 2008; Marwick 2008; Tufekci 2008). This concern, while well intentioned, is narrow. Steeves et al (2010: 4) notes that 'fears that children are at risk of sexual predation and/or harassment online are over-stated at best and subject to moral panic at worst'. Also, the focus assumes that children do not face the privacy risks which most concern adults (risks of fraud for

example). It also presumes that children are not inherently worried about their privacy and need adult intervention (Bryce and Klang 2009).

Fears for children's safety are invoked and amplified by commercial organisations selling software to allow parents to monitor, control or restrict children's internet use (Marx and Steeves 2010; Nolan, Raynes-Goldie and McBride 2011).[1] For example, the McAfee corporation states in their 'research' (serving as marketing): 'Do you know what your kids are doing online—whether they are talking to strangers or putting their computers and themselves at risk? Chances are, you know something about what your kids are doing on the internet but not everything' (McAfee 2010: 3). Educational initiatives and general information campaigns about young people and privacy also focus on online *safety*, most regularly teaching children and youth to protect themselves from online predators (Steeves et al. 2010), though also now often including a related form of predation, cyber-bullying by peers (see for example http://cybersmart.gov.au). The dominant understanding is that children are unable to negotiate or properly understand the idea and means of 'being private' online, compared with adults. However recent research suggests that not only do youth care about privacy (Tufekci 2008; Utz and Krämer 2009; Raynes-Goldie 2010), but that there is little difference between children's privacy attitudes and behaviours and those of adults (Lenhart 2009). Moreover, there is evidence that technical capacity (or at least techno-social familiarity) with social media *does* correlate with the capability to manage privacy protection (Brandtzæg, Lüders and Skjetne 2010).

As a more realistic understanding of children, privacy and risk emerges, perhaps we now need to frame new goals for privacy promotion and education, and new ways of helping children effectively act in ways which protect them. Withers and Sheldon concluded, as a key finding from major research into online privacy, that 'young people should be encouraged to create media texts … Creating their own media will enable young people to build greater critical skills towards information they access and create and learn more about the consequences of their actions online' (2008: 7). Furthermore, Steeves et al. (2010) suggest that privacy education needs to encourage children to think critically about how marketing and data mining shape their online experiences and that there are other dangers than those posed by some invisible 'strangers' (see also Nolan et al. 2011). How then might we proceed to develop among younger people effective, applied knowledge about the variety of risks they face online so as to keep them safe in all respects, while still able to take advantage of the very significant benefits of online interaction?

3. Autonomy through experiential learning games

According to Piaget, autonomy is 'the ability to think for oneself independent of reward and punishment, and to decide between right and wrong, and between truth and untruth' (as cited in Kamii 1991: 382). Research into developmental psychology shows that autonomy is strongly linked with a child's effective development with respect to identity formation and independence; responsibility; resilience; self-expression; pro-social behaviour; strong, trusting relationships; and critical thinking skills (see review in Nolan et al. 2011: 25-26). Such skills are vital to the development of healthy and effective understandings of privacy, for example the ability to assess properly who to trust or how to set appropriate interpersonal boundaries. Moreover, the development of autonomy and the related skill of self-control require the development of a sense of self that can serve as the locus for decision making about what to reveal of the self in public and thus for identity-forming social practices which in turn reinforce a sense of autonomy.

Experiential learning is classically defined as 'the process whereby knowledge is created through the transformation of experience' (Kolb 1984: 41). Such learning is effective because it 'relies upon an

[1] It is revealing that some of these products can infringe on privacy themselves, if in very different ways, by collecting data about the operations of individual users or by marketing additional services when installed (Grimes 2008a, 2008b; Marx and Steeves 2010).

engagement with social interactions and experience drawn from the "real world"' (de Freitas and Neumann 2009: 345). It is clear that 'although brain maturation plays a role, children's and adolescents' development of cognitive potentials depends on experience' (Larson and Angus 2011: 284). In respect of privacy-related decision making, experiential learning offers children a more effective way to learn to be autonomous than other approaches. Furthermore, instructional approaches based on the transmission of content to students from authorised adults would be counter-productive in producing the kind of cognitive and social skills needed to learn to be effective in privacy management. Chaille notes 'Educational experiences for young children should emphasize the construction of knowledge, not its transmission' (2003: 7). More specifically, 'By giving children opportunities to be independent, to make choices where appropriate, and to rely on themselves rather than on adults for materials and direction, we can greatly influence their sense of self, their confidence and sense of mastery, and their awareness of themselves as active constructors of knowledge—all aspects of being autonomous' (Chaille 2003: 8).

Itin has argued that:

> The educator's primary roles include selecting suitable experiences, posing problems, setting boundaries, supporting learners, insuring physical and emotional safety, facilitating the learning process, guiding reflection, and providing the necessary information.
>
> (1999: 93)

Such a position draws the important connection between learning from experience *and* the scaffolding of the learner's experience through the actions of a guide. In the normal use of scaffolding, the degree of support is reduced as learning proceeds, thereby increasing the autonomy of the learner in their educational experience. Vygotsky's zone of proximal development describes this situation: 'the distance between the actual developmental level as determined by independent problem solving and the level of potential development as determined through problem solving under adult guidance, or in collaboration with more capable peers' (1978: 86). In this model, the goal of educators is to provide children with learning experiences within this zone while providing the appropriate support or scaffolding.

John Pijanowski (drawing on Bransford Brown and Cocking 2000), describes some of the practical activities involved in scaffolding:

> interesting the student in the task; reducing the number of steps required to solve a problem by simplifying the task, so that a student can manage components of the process and recognize when a fit with task requirements is achieved; maintaining the pursuit of the goal, through motivation of the student and direction of the activity; marking critical features of discrepancies between what a student has produced and the ideal solution; controlling frustration and risk in problem solving; and demonstrating an idealized version of the act to be performed.
>
> (Pijanowski 2009: 7)

One challenge is to create experiences realistic enough to constitute an engagement with the real world but which also permit the kind of scaffolding necessary to make experiences more than *just* experiences, allowing the transformative process by which they become knowledge. Furthermore, in working with younger children—especially in a risk-laden context such as online privacy—there needs to be significant distance between reality and the authentic recreation of that reality for the purposes of learning. It is true that 'when children in our society live in a literate world in which many signals for reading, writing, investigating and mathematics are available, children are motivated to meet this world of adults' (van Kuyk 2011: 137); but in learning about online privacy, the purpose is to avoid too early contact with 'the world of adults' until sufficient skills have been learned. So, if adult education often labours to make learning sufficiently authentic (Herrington and Herrington 2006), in the case of young children, the

challenge is to avoid *too much* authenticity while still having an experience appropriate to the application of the knowledge gained.

Games provide the answer to this challenge. The use of games as platforms for experiential learning has been explored by a number of researchers (discussed in Kiili 2005b), particularly with respect to so-called 'serious' games for change (Westera et al. 2008; Charsky 2010). By games, we do not mean 'drill and practice' (Charsky 2010: 178), but social games which deliberately involve experiential learning, with an 'integration of game-play and pedagogy' (Kiili 2005a: 17) through cycles of action and reflection, and exploration of different outcomes based on different inputs. Such games subtly include through their design the scaffolding needed for learning. Games also have key qualities necessary for learning about privacy at an early age. Miller and colleagues show how the 'signature pedagogy' (Shulman 2005: 52) of early education emphasises children 'being encouraged to take responsibility for themselves and their actions' (2012: 232). They conclude that that when children playing games are 'facing challenges, communicating, learning and applying skills, reframing their understanding on the basis of feedback, and so on', such games motivate learning and scaffold it effectively, in part because of the social interaction between players (2012: 234-235). Finally, the simulation aspect of games (e.g. Hofstede, De Caluwé and Peters 2010) has proven effective to create safe experience-based learning for younger children, allowing difficult concepts and contexts to be sufficiently constrained. Ultimately, in game play, what children can simulate is the life world of adult decision-making and, from that, learn experientially how best to become safely part of that world.

4. Game design as participatory action research

Privacy in online interaction is a complex area whose specific working for younger children is still not well understood, especially in relation to the management of information sought by commercial organisations. Further, it would appear an experiential game could usefully educate children to manage better their privacy autonomously. The research method that best suits exploration of this situation is action research, involving the co-creation of a game, with an embedded research process aimed at both informing game development process, but also in providing some initial understanding of privacy attitudes among young children, which is a largely unexplored area of research (Nolan and Weiss 2002; Jenson, De Castell and Bryson 2003; Nolan and Sponaas-Robins 2006; Bal and Combès 2006; Raynes-Goldie and Walker 2008; Nolan, Mann and Wellman 2008; Boler 2008; Nolan and Bakan 2009; Nolan 2010; Raynes-Goldie 2010a). To this end, the project took on two stages. In the first stage, we sought to discover what children already knew about online privacy; how they have been engaged by education; and what they felt was important to teach *other* children. The findings from this initial exploration then informed the second stage of the project—the design of the game as an applied outcome of the process. Given the emphasis on autonomy, children were co-creators of the game, participating *in* the research and solving the real-world problems of learning about privacy (see O'Brien 2001). The children were participants throughout the game design process (Edwards and Alldred 1999), co-constructing a shared understanding of the game, its learning goals and the broader research findings with the children (Anderson, Gentile and Buckley 2007). Such a method allowed a more equal engagement between researchers and participants.

Participants, aged roughly between eight and ten, were recruited from community groups such as GamerCamp Jr. and TIFF Nexus in Toronto, Canada, using word-of-mouth recruitment to seek five male and five female participants. Work commenced with four girls and five boys but due to unforeseen circumstances, the final participant group consisted of two girls and five boys, aged between eight and eleven. These children participated in a two-stage series of discussions, hands-on workshops, game playtest and feedback sessions. In the first stage, the researchers and the co-creators established what they already knew about privacy, what they wanted to know more about and what they felt other children should learn. This data from this phase then informed the game development in the second stage. In the second phase, which focused on game development, the co-creators learned the basics of game design so

they could be active in the research and design process.[2] The game was then was iteratively co-designed through five prototypes to a finished product, focusing not just on how engaging it was to play, but also providing some initial findings with respect to its efficacy at developing skills in privacy management by children. The co-creators were central to the graphic and conceptual design of the game, including the 'world' in which play takes place, the type and nature of characters as well as their graphical representations.

Throughout all stages of the project, data was collected by studying the individuals in the actual process of design, producing thick descriptions of relationships and actions (Machin 2002), as well as collaborative facilitation techniques (Gunn 2008) and storytelling (Davis 2007). Group discussions about privacy, the game design process and playtest feedback sessions were recorded via written notes, audio recordings, still photographs and some video recording. Research and game design notes from group discussions and playtests were created collaboratively and shared and records kept.

The first stage of the project involved explicit discussion of the nature of privacy, online activity and the children's experiences with the internet, so as to inform the design of the game. In these discussions we explored with our co-creators many of the different aspects of privacy while carefully avoiding the use of the term itself. We therefore attempted to ground the development of the concept in the children's own experiences and knowledge, noting that, even for adults, 'privacy' is a very difficult notion to define (Solove 2007: 8). While there was no consensus for a singular notion of privacy, our discussions showed that children were well aware of the value of privacy and, accordingly, took steps to protect it, whether in a physical space (such as a bedroom) or a virtual one (for example, using avatars that did not reflect actual appearance).

All the co-creators bar one reported that adults had told them to be concerned about their online privacy, particularly in terms of 'stranger danger'. However they said that had not been told that online companies might use their information, and had not been taught how to make choices about when or if to trust websites or online games. But the children were already aware of protecting themselves from institutional surveillance. One co-creator noted that the agreements needed to sign up for a game were not there to protect children but rather protected companies 'from being sued'. Another evaluated the trustworthiness of sites based on the length of their Terms of Service agreements. While this evaluation tool may not be effective, it is clear evidence that children think critically about the privacy issues involved in using games online.

Our co-creators were already familiar with commercial services whose use might give rise to privacy concerns. They regularly played online games such as Monkey Quest (reported by five participants), Moshi Monsters (four), Club Penguin (five) and Webkinz (five). One co-creator also reported using a wiki (after getting his mother's permission), while another used his mother's account to play Farmville. Five co-creators reported they used Bitstrips, a site where people make and share comics. One was also heavily involved in Flipnote Hatena, an all-ages site to share Nintendo DS animations.[3] Notably, we observed that children had broad notions of privacy that were expressed in terms of *online* privacy (as if the two were no different). During the workshops, they would frequently discuss broader issues only through experiences or thoughts relating to the online games they played, for example their concern at seeing a friend's account being hacked or their frustrations with 'greedy' online game companies.

[2] The curriculum was based on Schell's (2008) *The Art of Game Design* and Woo's GamerCamp Jr. Activity Kits. These kits can be downloaded from http://gamercampjr.com/gamemaking-kits/

[3] Near the end of the project, she created a trailer for the game entirely on her own using Flipnote Hatena: http://gamingprivacy.org/2012/01/a-trailer/

In the second stage of the project, the researchers and co-creators worked together to create a privacy literacy game that focused on the key areas that had been identified in the first stage. A crucial element in the research and design process was the iterative development of heuristic guidelines by which children could make judgements of what risks might be taken and what trust should be placed in others. Such judgements are central to the ongoing, effective negotiation of privacy online. The guidelines, therefore, were central to the design of the game and, through play, the game would enable players to practise making these judgements. The guidelines were based on feedback from play-tests and group discussions, read through a context of decision making, learning theory and strategic planning, such as Pijanowski's (2009) framework for developing a moral decision-making curriculum. The guidelines encompassed three basic stages of decision making: information gathering; assessment of pros and cons; and critical reflection, set in the context of websites, online games and other internet services. For example, in gathering information we suggested 'Asking teachers, parents, or librarians' or 'asking friends'; in the second stage, using the information gathered, questions could be asked such as 'What is the motivation or goal of the game or website? How might that affect me and my private information?' In the third stage, the questions drew out the knowledge from the experience: 'What happened as the result of my choice to use or not use the game or website?' These heuristic rules for judging privacy risk and trust were embedded in game-play so as to make them 'experienced' rather than 'taught'.

5. *The Watchers*: A privacy literacy game

The Watchers, a computer game/board game hybrid, was the result of the participatory co-research and co-design process just described. Both the board-game components and software are downloadable for free from the game website (http://watchersgame.com).[4] *The Watchers* is played much like a conventional board game where a group of players interact with each other and the game while gathered around a table. Augmenting this play is the computer-game element, using a shared computer or tablet. The game software provides players an initial game tutorial and then guides them through the game itself, showing the progression of the game narrative and giving players feedback about the consequences of their actions. This computer-based element increases game immersion and narrative development in a way not possible with a board game alone. However, the collaboration demanded by sitting together at a table enables social and play interaction otherwise difficult to achieve with just a computer game.

The Watchers is set in the fictional 'Union City', a city on the intersection of seven different 'universes'. In this city, species from the universes live together. Tasked with protecting the city is a secret government organisation, 'the Watchers'. Players take on the role of secret agents, one from each dimension, working together to solve mysteries and save the city from disaster. Union City has a very important feature: a computer network called Hatnet which citizens access via telepathic links in their hats. Hatnet is the key educational element in the game. It is, of course, a version of the internet and therefore serves as the basis for the learning outcomes around online privacy. However, the whole purpose of the game is to make this version *unlike* the internet. Hatnet was designed to implement the Russian Futurist notion of creating critical distance through defamiliarisation, opening up familiar things for investigation and better understanding by making them strange (Bigge 2006). Crucially, therefore, and in order to maintain the illusion of difference which is required for greater comprehension, Hatnet is *never* compared to the internet in the game. Indeed, the internet is never mentioned at all. Hatnet makes sense inside the non-real setting. It is consistent *with* the game, and equivalent *to* the real-world learning focus. Thus, in the game, there is a version of Facebook, called Puffbook. This distance from reality produces the possibility of experiential learning through exploration and discussion of that distance. At the same time, especially for younger players, it makes the concepts to be learned more accessible.

[4] The board-game component is easily printable and assembled using a standard printer, paper, scissors and tape. The board game is also available in a professional printed version which can be ordered at cost on the game website.

The game has three different episodes, each of which contains three missions to be completed. Each episode explores basic concepts of why and how internet-based games and websites collect and utilise personal information. The specific concepts explored are data shadows (the information we put online remains, like a shadow, yet not easily seen); information gathering and aggregation by large companies; and the use of personal information for marketing purposes. These missions and episodes use the well-established concept of game levels: the first mission is the easiest, with the greater difficulty as players move from one mission to the next. Each episode is a self-contained experience, with its own story but, as players progress from one episode to the next, they work with ideas, characters and plots from the previous episodes which are all part of an overarching narrative. The mission / episode approach builds in rewards for effective learning since, until the problem in each level is solved, players cannot progress. The episodic structure and overarching narrative enables a deeper experience where players are actively engaged with the story and characters. The narrative encouraged continued advancement through the game. The use of this mission / episode structure also allowed creation of the scaffolding necessary for effective experiential learning as well as to create specific subsidiary learning outcomes, whose achievement then enables deeper learning in future. This scaffolding is concealed, enabling players to learn while not realising they are doing so, employing the concept of immersion in game-play, a common trait of successful learning games (Kiili 2005b).

In each mission, players must work together as a team to solve mysteries in Union City; the game-play involves gathering and using information to solve each mystery. The game reveals over time how these events are related, though this is not clear at first to players. For example, in the first episode, the Watchers must solve a case where Hatnet users find that unwanted, duplicate avatars of themselves are appearing. These avatars wreak havoc on the city, inundating people with unwanted advertisements. As the missions unfold, players learn that the duplicates were inadvertently created by the collection of personal information from Hatnet users. Over the next two episodes, it is gradually revealed that these duplicates were part of a larger plan by a company named Zongog to gather and analyse personal information about everyone in the city in order to sell a highly addictive toy.

The three-stage guidelines discussed above are crucial in helping players to learning how these concepts work and the need for thoughtful decision-making. In each mission, the first stage of solving the mystery is to gather information. The game begins with six investigation cards placed on the game board. Players travel around the board, collecting ability cards (research, intuition, observation and conversation) which they use to unravel the mystery. For example, in the third episode, the players must find a way to contact the CEO of Zongog. The players are given a number of options including: sneaking into the Zongog headquarters; sending a message to the CEO on LinkedUp (a version of LinkedIn); or paying a Zongog insider to facilitate the message. Through their investigations, players uncover the various pros and cons of each action. These investigations comprise a standard set of three choices: analysing an agreement; asking an informant; or researching history. For example, asking an informant about sneaking into the Zongog headquarters reveals to players that it is very difficult to sneak in without being seen, and as a consequence, everyone on the team would lose some game resources. This set of choices, based our heuristic guidelines, are transferable to real-world assessments of online services. For example, the 'researching history' option aligns with researching the past activities of an internet company, like Facebook, in its treatment of users; 'analysing an agreement' models the act of reading the Terms of Service or privacy policy of an online game.

We discovered an important part of practising and engaging with the guidelines was through social interaction and collaborative assessment. Thus, team-based discussion and co-ordination are another important aspect of *The Watchers*. The players have to work together to plan how best to investigate each mystery, while managing the group's shared resources. Goals are reached as a team and not through individual players competing with one other. Even though the game-play is largely based on individual turns, the players can plan together what each person will do on their turn for the best collective outcome.

In addition to this informal process, evident in how the game was played by our participants, each episode requires a formal discussion of outcomes. Each player presents their choice of the best action to take to the group based on the information gathered. The group then deliberates and decides which choice to take. These choices have consequences in later missions. For example, if the team chooses to engage in questionable activities, such as hacking into a database or another action that might threaten someone else's privacy, their reputation or whuffie decreases.[5] As a team's whuffie decreases, so does the willingness of characters in the game to help the team, making future investigations more difficult. This interaction between choices, actions and consequences completes the three-stage approach by enabling players to reflect on the relationship between actions and outcomes.

The game mechanics mirror and reinforce the narrative of the game. Just as the potential pros and cons of various actions are uncovered through the game's storyline when players complete investigations, the game's mechanics encourage the same sort of critical thinking, deliberation and teamwork. The currency of the game—infobux—is held by the team rather than individual players and some actions require its use, thus requiring discussion with the group. In contrast, ability cards, required to complete investigations, are collected and held by individual players. But, completing an investigation requires the right combination of Ability cards—a combination rarely held by a single player. Players can share cards, but only under certain circumstances, and there is also a limit on the number of rounds the team has to complete an investigation. Thus, to succeed, players must work together to plan an optimal approach for their individual actions, balancing the risks and rewards of any specific approach.

6. Conclusions

Designing, improving and playing *The Watchers* has shown the possibilities of achieving a successful learning outcome about technology, through technology, when children's own perspectives and experiences are taken into account, as well as their approach to play and learning through play. Through careful game design, scaffolding for experiential learning was included to guide their development of autonomous skills in managing privacy as well as creating a simulation both strange and familiar necessary to engage their attention and make for a safe learning experience.

The learning goal of the game was, broadly, to increase players' abilities in everyday life to assess risks to privacy and make appropriate judgements about when, what and who to trust. The aim was to enhance children's autonomy through their ability to control their privacy better in online contexts. Throughout the research and design process we emphasised these outcomes and tested the degree to which we were succeeding. We gained insight into the game's design and success through direct feedback from the co-creators via discussions before and after playing, and through observation during play-test sessions. In these sessions, the children discussed the choices they had made and assessed different results. One notable outcome was that, without adult prompting, the co-creators began integrating this kind of debate into their game-play during the playtests. It was decided that this process should become *part* of the game itself and so, in later versions of the game, the debate process was made a necessary part of the end of each episode. The process of design suggested that children have a strong sense of the benefit of social interaction and collaborative assessment as a means for learning about privacy-oriented behaviour and value that interaction with peers as a key problem solving technique.

The game also related to the everyday decisions children make online. In a final feedback session we asked the co-creators if they felt the skills they developed in the game could be applied to 'real life'. One of them replied 'One of the things I do before I want to join an online game is Google it first and I see what people are saying....' We asked the group 'What [game category] might that fall under?' One replied

[5] A term borrowed from Cory Doctorow's *Down and Out in the Magic Kingdom* (2003), where it is essentially used to describe social capital.

'Ask informants' to which the original co-creator added, 'It would fall under ask informants or research history... because people talk about it on the internet as well as just write about it on the internet and say "Oh this is a good game"'. There were similar comments from other co-creators about this specific aspect of the game, as well as more broadly, such as that '[the game shows that] you have to look carefully at actions before you choose', or that it shows 'how to trust people and websites, look at the consequences of what you're agreeing to'.

One co-creator reflected on his experience by saying that the game helped him to understand the privacy consequences of using online games but did not tell him how to 'solve the consequences'. The challenge he expressed was that truly protecting privacy online can mean opting out entirely, which is neither ideal (given the benefits of online interaction) nor realistic (given the social expectations to engage in this behaviour). The game, in our view, can therefore help to develop a critical awareness of the *challenges* of privacy, not just the techniques involved in managing it. At the same time, the children reported that the game helped them to work together as a team and that they improved their discussion and negotiation skills. One of the co-creators said that it helped him to learn how to convince other people of his ideas and we also observed these skills during our play-test sessions. While not immediately related to privacy, learning these skills in the context of a privacy-oriented game suggests that privacy management by children can be enhanced by the more general development of their cognitive and social skills, enabling them to rely on (and help) others with challenges.

The logistics of the project also point to some important directions and considerations for future research, particularly with respect to further evaluation. Due to the scope of the project, imposed by the logistical realities of working with children, it was only possible to work with one group of children. The result of this is a degree of limitation in early feedback and testing for the game, as the children who co-created it were also its first evaluators. Thus, the researchers hope to develop a second phase of the project with second group of children to allow for a deeper evaluation and refining of the game.

Ultimately, the research and design process for *The Watchers* suggests two key considerations for the authorities (parents and institutions) who are rightly charged with the responsibility of keeping children safe while also allowing them to learn how autonomously to take care of themselves. Firstly, as experienced repeatedly in the process of discussing privacy while designing the game, children are not the naïve experts imagined by some public discourses. By treating children as partners in learning (as in the game design process), adults are much more likely to connect with the concerns they have and develop with them effective approaches to privacy management. Second, the research suggests the efficacy of games as the locus for simulated experiential learning, where the skills learned and decisions to be made experiences are as real as can be, but the environment is sufficiently unfamiliar to both engage the children's sense of play and also make them think explicitly about activities that might otherwise be tacit. This combination of taking children seriously as partners in learning, but through the medium of games (normatively understood to be not serious) creates a useful combination by which to address the important concerns of allowing children to work out how they themselves can be safe online.

Acknowledgements

This research paper was developed as part of *Gaming Privacy*, a joint project between Atmosphere Industries and Ryerson University's Experiential Design and Gaming Environments lab. The project was generously funded by the Office of the Privacy Commissioner of Canada's Contributions program with additional support from Ryerson University. The authors gratefully acknowledge the research input and support of Noah Kenneally, Jaime Woo, Jason Nolan, Melanie McBride, and Sara Grimes. The authors also wish to thank David Fono, who co-led the game design process as well as Dara Gold, Nick Pagee, Rhett Fester, Adrian Hon, Niki Chaplin, Adam Clare, Alex Raynes-Goldie, and Sagan Yee for their game development support. The authors most especially wish to thank the project's team of co-researchers and game co-creators, Chris, Jordan, Kiri, Mary, Mitchell, Peter and Tinson.

References

Albrechtslund, A. 2008. Online Social Networking as Participatory Surveillance. *First Monday* 13 (3). http://firstmonday.org/article/view/2142/1949

Anderson, C. A., D. A. Gentile, and K. E. Buckley. 2007. *Violent Video Game Effects on Children and Adolescents: Theory, Research, and Public Policy.* New York: Oxford University Press.

Bal, A. and Y. Combès. 2006. Les Campus Numériques au Carrefour d'Enjeux Pédagogiques, Industriels et Institutionnels [Digital Campuses and the Intersection of Pedagogical, Industrial and Institutional Issues]. *Etudes de Communication, Dossier : L'intégration du Numérique dans les Formations du Supérieur*,1: 56-75. Available at: http://imagearts.ryerson.ca/abal/pr/erte_final.pdf

Barnes, S. B. 2006. A Privacy Paradox: Social Networking in the United States. *First Monday* 11 (9). http://firstmonday.org/article/view/1394/1312

Baym, N.K. and d. boyd. 2012: Socially Mediated Publicness: An Introduction. *Journal of Broadcasting & Electronic Media* 56(3): 320–329. http://dx.doi.org/10.1080/08838151.2012.705200

Bigge, R. 2006. The Cost of (Anti–)Social Networks: Identity, Agency and Neo–luddites. *First Monday* 11 (12). http://firstmonday.org/article/view/1421/1339

Boler, M. 2008. *Digital Media and Democracy: Tactics in Hard Times.* Cambridge: MIT Press.

boyd, d. and H. Jenkins. 2006. *MySpace and Deleting Online Predators Act (DOPA). MIT Tech Talk.* May 26. http://www.danah.org/papers/MySpaceDOPA.html

Brandtzæg, P. B., M. Lüders and J. H. Skjetne. 2010. Too Many Facebook 'Friends'? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *Journal of Human–Computer Interaction* 26 (11–12): 1006–1030. http://dx.doi.org/10.1080/10447318.2010.516719

Bransford, J., A. Brown and R. Cocking. 2000. *How People Learn: Brain, Mind, Experience, and School.* Washington: National Academies Press.

Bryce, J. and M. Klang. 2009. Young People, Disclosure of Personal Information and Online Privacy: Control, Choice and Consequences. *Information Security Technical Report* 14 (3): 160–166. http://dx.doi.org/10.1016/j.istr.2009.10.007

Chaille, C. 2003. *The Young Child as Scientist: A Constructivist Approach to Early Childhood Science Education.* Boston: Allyn and Bacon.

Charsky, D. 2010. From Edutainment to Serious Games: A Change in the Use of Game Characteristics. *Games and Culture* 5 (2): 177–198. http://dx.doi.org/10.1177/1555412009354727

Davis, P. 2007. Storytelling as a Democratic Approach to Data Collection: Interviewing Children about Reading. *Educational Research* 49 (2): 169–184. http://dx.doi.org/10.1080/00131880701369693

Debatin, B., J. P. Lovejoy, A.–K. Horn and B. N. Hughes. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer–Mediated Communication* 15 (1): 83–108. http://dx.doi.org/10.1111/j.1083–6101.2009.01494.x

de Freitas, S. and T. Neumann. 2009. The Use of 'Exploratory Learning' for Supporting Immersive Learning in Virtual Environments. *Computers & Education* 52 (2): 343–352. http://dx.doi.org/10.1016/j.compedu.2008.09.010

Doctorow, C. 2003. *Down and Out in the Magic Kingdom.* New York: Tor Books.

Dwyer, C., S. Hiltz and K. Passerini. 2007. Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *AMCIS 2007 Proceedings.* Paper 339. http://aisel.aisnet.org/amcis2007/339

Edwards, R. and P. Alldred. 1999. Children and Young People's Views of Social Research. *Childhood* 6 (2): 261–281. http://dx.doi.org/10.1177/0907568299006002007

Grimes, S. 2008a. I'm a Barbie Girl in a BarbieGirls World. *The Escapist.* http://www.escapistmagazine.com/articles/view/issues/issue_165/5187-Im-a-Barbie-Girl-in-a-BarbieGirls-World

Grimes, S. 2008b. Kids' Ad Play: Regulating Children's Advergames in the Converging Media Context. *International Journal of Communcations Law & Policy* 12: 161-178. http://ijclp.net/old_website/article.php?doc=8&issue=12_2008

Gunn, A. 2008. Creating Participatory Events. *Aspiration*. http://www.aspirationtech.org/files/AspirationCreatingParticipatoryEvents.pdf

Herrington, J. and A. Herrington, eds. 2006. *Authentic Learning Environments in Higher Education*. Hershey, PA: IGI Global.

Hofstede, G. J., L. De Caluwé and V. Peters. 2010. Why Simulation Games Work–In Search of the Active Substance: A Synthesis. *Simulation & Gaming* 41 (6): 824-843. http://dx.doi/org/10.1177/1046878110375596

Itin, C. 1999. Reasserting the Philosophy of Experiential Education as a Vehicle for Change in the 21st Century. *Journal of Experiential Education* 22 (2): 91–98.

Jenson, J., S. De Castell and M. Bryson. 2003. 'Girl Talk': Gender, Equity, and Identity Discourses in a School–based Computer Culture. *Women's Studies International Forum* 26 (6): 561-573. http://dx.doi.org/10.1016/S0277-5395(03)00124-9

Kamii, C. 1991. Toward Autonomy: The Importance of Critical Thinking and Choice Making. *School Psychology Review* 20 (3): 382–388.

Kiili, K. 2005a. Digital Game–based Learning: Towards an Experiential Gaming Model. *The Internet and Higher Education* 8 (1): 13–24. http://dx.doi.org/10.1016/j.iheduc.2004.12.001

Kiili, K. 2005b. *Educational Game Design: Experiential Gaming Model Revised.* Tampere University of Technology.

Kolb. D. 1984. *Experimental Learning.* Englewood Cliffs, NJ: Prentice–Hall.

Larson, R. W. and R. M Angus. 2011. Adolescents' Development of Skills for Agency in Youth Programs: Learning to Think Strategically. *Child Development* 82 (1): 277–294. http://dx.doi.org/10.1111/j.1467–8624.2010.01555.x

Lenhart, A. 2009. *Adults and Social Network Websites*. Pew Internet and American Life Project. http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx

Livingstone, S. 2006. Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. In *Computers, Phones and the Internet: Domesticating Information Technology*, edited by R. Kraut, M. Brynin and S. Kiesler, 128–144. Oxford: Oxford University Press.

Machin, D. 2002. *Ethnographic Research for Media Studies.* London: Arnold.

Marwick, A. E. 2008. To Catch a Predator? The MySpace Moral Panic. *First Monday* 13 (6). http://firstmonday.org/article/view/2152

Marx, G. and V. Steeves. 2010. From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society* 7 (3/4): 192–230. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4152

McAfee 2010. *The Secret Online Lives of Teens*. Santa Clara: McAfee. http://us.mcafee.com/en–us/local/docs/lives_of_teens.pdf .

Miller, D., D. Robertson, A. Hudson and J. Shimi. 2012. Signature Pedagogy in Early Years Education: A Role for COTS Game–Based Learning. *Computers in the Schools* 29 (1–2): 227–247. http://dx.doi.org/10.1080/07380569.2012.651423

Nolan, J., S. Mann, and B. Wellman. 2008. Sousveillance: Wearable and Digital Tools in Surveilled Environments. In *Small Tech: The Culture of Digital Tools*, edited by B. Hawk, D. Rieder and O. Oviedo, 179-196. Minnesota: University of Minnesota Press.

Nolan, J., K. Raynes–Goldie, and M. McBride. 2011. The Stranger Danger: Exploring Surveillance, Autonomy and Privacy in Children's Use of Social Media. *Canadian Children: Journal of the Association for Young Children* 36(2): 24-32.

Nolan, J., and R. Sponaas–Robins. 2006. Collaborative Text–Based Virtual Learning Environments. In *The International Handbook of Virtual Learning Environments*, edited by J. Weiss, J. Nolan, J. Hunsinger, and P. Trifonas, 429-438. Berlin: Springer.

Nolan, J. and J. Weiss. 2002. Learning Cyberspace: An Educational View of the Virtual Community. In *Building Virtual Communities: Learning and Change in Cyberspace*, edited by K. Renniger and W. Shumar, 293–320. Cambridge: Cambridge University Press.

Nolan, J. 2010. Learning With Anne: Early Childhood Education Looks and New Media for Young Girls. In *Anne of Green Gables: New Directions at 100*, edited by I. Gammel and B. Lefebvre, 117-133.Toronto: University of Toronto Press.

Nolan, J. and Bakan, D. 2009. Social Technologies for Young Children: Cultural Play with Songchild.org. In *Toronto/Montréal/Lille: Together Elsewhere*, edited by L. Poissant and P. Tremblay, n.p. Montréal: Presse de l'Université du Québec.

O'Brien, R. 2001. Um Exame da Abordagem Metodológica da Pesquisa Ação [An Overview of the Methodological Approach of Action Research]. In *Teoria e Prática da Pesquisa Ação [Theory and Practice of Action Research]*, edited by Roberto Richardson, n.p.. João Pessoa, Brazil: Universidade Federal da Paraíba. (English version) Available: http://www.web.ca/~robrien/papers/arfinal.html

Pijanowski, J. 2009. The Role of Learning Theory in Building Effective College Ethics Curricula. *Journal of College and Character* 10 (3): 1–13. http://dx.doi.org/10.2202/1940-1639.1088

Rainie, L. and B. Wellman. 2012. *Networked: The New Social Operating System* Cambridge, MA: MIT Press.

Raynes–Goldie, K. 2010. Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook. *First Monday* 15 (1). http://firstmonday.org/article/view/2775/2432

Raynes–Goldie, K. 2011. Annotated Bibliography: Digitally Mediated Surveillance, Privacy and Social Network Sites. Paper presented at Cybersurveillance and Everyday Life: An International Workshop, Toronto May 12-15.

Raynes-Goldie, K. and L. Walker. 2008. Our Space: Online Civic Engagement Tools for Youth. In *Civic Life Online: Learning How Digital Media Can Engage Youth* edited by W. Lance Bennett, 161–188. Cambridge, MA: The MIT Press. http://dx.doi.org/10.1162/dmal.9780262524827.161

Schell, J. 2008. *The Art of Game Design: A Book of Lenses.* Burlington, MA: Morgan Kaufmann.

Schrammel, J., C. Köffel and M. Tscheligi. 2009. How Much do You Tell? Information Disclosure Behaviour in Different Types of Online Communities. In *C&T '09: Proceedings of the Fourth International Conference on Communities and Technologies*, 275–284. New York: ACM. http://dx.doi.org/10.1145/1556460.1556500

Shulman, L. S. 2005. Signature Pedagogies in the Professions. *Daedalus* 134 (3): 52–59. http://www.mitpressjournals.org/doi/abs/10.1162/0011526054622015

Solove, D. J. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review* 44: 745.

Steeves, V., T. Milford and A. Butts. 2010. *Summary of Research on Youth Online Privacy*. Ottawa: The Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/information/pub/yp_201003_e.pdf

Tufekci, Z. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society* 28 (1): 20–36. http://dx.doi.org/10.1177/0270467607311484

Utz, S. and N. Krämer. 2009. The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace 3*2. http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

van Kuyk, J. J. 2011. Scaffolding – How to increase development? *European Early Childhood Education Research Journal* 19 (1): 133–146. http://dx.doi.org/10.1080/1350293X.2011.548965

Vygotsky, L. S. 1978. *Mind in Society: The Development of Higher Psychological Processes.* Cambridge: Harvard University Press.

Westera, W., R. J. Nadolski, H. G. K. Hummel and I. Wopereis. 2008. Serious Games for Higher Education: A Framework for

Reducing Design Complexity. *Journal of Computer Assisted Learning* 24 (5): 420–432. http://dx.doi.org/10.1111/j.1365-2729.2008.00279.x

Withers, K. with R. Sheldon. 2008. *Behind the Screen: The Hidden Life of Youth Online*. London: Institute for Public Policy research. http://www.ippr.org/images/media/files/publication/2011/05/behind_the_screen_1632.pdf