THE SCOOP: HOW TO PROTECT YOUR DIGITAL PRIVACY IN THE AGE OF SURVEILLANCE CAPITALISM

By

Yerachmiel (Jeremy) Paquette

Bachelor of Fine Arts in Performance Production, Ryerson University, 2017

A Major Research Project

presented to Ryerson University

in partial fulfillment of the requirements for the degree of

Master of Digital Media

in the program of

Digital Media

Toronto, Ontario, Canada, 2020

Author's Declaration

I hereby declare that I am the sole author of this MRP. This is a true copy of the MRP, including any required final revisions. I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research. I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my MRP may be made electronically available to the public.

THE SCOOP: HOW TO PROTECT YOUR DIGITAL PRIVACY

IN THE AGE OF SURVEILLANCE CAPITALISM

Master of Digital Media, 2020

Yerachmiel (Jeremy) Paquette

Digital Media

Ryerson University

Abstract

The perception of Generation Y as "digital natives", whose very minds have been shaped by the technology they were raised alongside (Prensky, 2001), is increasingly under fire. Many young adults struggle with anything more than basic operation of technology, and lack the digital literacy to find and discern accurate information on the Internet. In an environment of increasing surveillance and malicious intrusion into corporate and personal data, there can be severe consequences to this skill gap. However, because of the assumption of competence attached to Generation Y, accessible post-educational resources are scarce for those outside of specific technology-related fields. This project aims to create a game which will serve as a stepping-stone for those interested in gaining knowledge and empowering themselves to take control of their digital lives. By presenting real-world scenarios of gradually increasing complexity, through gameplay environments focused on strategy and careful decision-making, digital literacy and security skills can be built from the ground up to serve as a foundation for further research and the development of secure personal habits.

Keywords: Digital literacy, digital natives, information security, Generation Y, millennials, educational games

Acknowledgement

I want to acknowledge two people for their support in completing this MRP. First, my advisor Michael Bergmann, who has been an incredible teacher and the person I turn to for career support since we first met in 2017. Without his support in both my undergraduate and now graduate programs, it is doubtful I would have achieved what I have so far. And second, but no less, I need to thank Michael Smilovitch not only for his help as a second reader, but also for his patience and passion while introducing our class to video game development last semester. This project would have run aground immediately without the experience I gained in his course.

Dedication

This MRP, and my master's degree, are dedicated to my wife Paris.

No matter where she is in the world, I am never alone.

אשת חיל מי ימצא ורחוק מפנינים מכרה

Table of Contents

List of Figures

List of Appendices

Introduction

The generation born during the rapid advance of technology in the decades of change and progress leading up to the new millennium has been termed “digital natives”. Raised during the creation of the World Wide Web, the millennial generation were believed to be “native speakers of the digital languages of computers, video games and the Internet” (Prensky, 2001, p. 1). However, as these children entered all levels of the education system, it became clear that familiarity with the basic operation of the devices in their everyday lives—computers, televisions, and video game consoles—did not translate to a deeper level of digital literacy and technical skill (Sherry & Fielden, 2005; Calvani et al., 2010; Li & Ranieri, 2010).

The impact of this gap in knowledge is potentially far-reaching. Digital literacy includes not just rote technical ability, but also an individual’s capacity to participate in online communities, search for information, and critically assess information presented to them (Eshet-Alkalai, 2004). Early deficiencies in these areas show some tendency to self-reinforce, meaning that a user who has negative experiences with technology comes to see themselves as “not tech-savvy”. This reduces self-efficacy and limits the person’s overall lifetime experience with information technology (Zimic, 2010). Poor digital literacy skills have both individual effects—lower productivity at work, falling victim to scams, or paying high prices for a technician to perform basic computer maintenance—and societal effects. The recent past has demonstrated that millions of individuals without sufficient digital literacy can contribute to electoral manipulation, and modern political discussions increasingly involve regulation of technology companies, data privacy and protection, the legality of encryption, and other issues with global impacts.

This major research project aims to build an educational game to improve digital literacy among millennials. Educational games have been used extensively in classrooms since the introduction of computers to the school environment, and a solid foundation of pedagogical principles exists to support their use. For example, Sauvé et al. (2010) present meta-evidence that video games aid in the development of structured knowledge and problem-solving skills, both key to digital literacy. In the simulated world of a video game, students can act as they would in

the real world, but suffer none of the consequences of an incorrect decision. This allows for multiple iterations of the problem-solving process to occur quickly, without incurring the financial or psychological costs of real-world failure. If the game allows it, players can save their progress, test a solution, and reload the game if the solution is not as effective as predicted. Assessment can be performed both immediately through real-time feedback within the game, and later through analytics gathered while playing. The accessibility of video games also makes the format suitable for a distributed educational effort, freely available on the Internet to anybody who wants it, as opposed to a scheduled in-person or online class.

The first phase of this project, and the one described in this paper, is an educational game designed to teach the various aspects of protecting personal data from both malicious and passive intrusion. "Surveillance capitalism" has arisen as a term for describing the almost indiscriminate collection of user data for marketing, analysis, and behavioural prediction. These practices are driven by globally famous tech companies like Google, Amazon, Microsoft, Facebook, along with countless thousands of other minor data-aggregation firms which sell their data to businesses and to larger players. Zuboff (2015, p. 75), who coined the term "surveillance capitalism", identifies this data collection not as an isolated trend driven by technological capability, but as part of the logic of accumulation which drives capitalism itself. More data is better—and since the cost of storage continues decreasing year over year, no piece of information is too minor to collect and store. Regulation may rein these companies in in the short term, but users are hungry for "free" services, and happy to pay the price with their data. However, researchers like Wang and Herrando (2019) and Mendes (2018) demonstrate that millennials do indeed care about their online privacy and security, at least on paper, even if these preferences do not always translate into more effective digital security behaviours (Jiang et al., 2016). If the idea of individual privacy and control over one's own data is to be preserved before it becomes archaic, effort is needed to educate current and future generations of consumers.

The topic was chosen by a small informal survey of millennials who rated themselves as less technologically familiar. Most commonly, those who were surveyed perceived privacy and data loss as a serious issue, but one they were largely unfamiliar with the nuances of. For example, one individual was surprised to learn that Facebook can track users through cookies

which are read by the social sharing buttons found on most web sites. The impact of the game is entirely dependent on self-motivation by participants, which can be assisted by good game design but fundamentally relies on a topic which resonates with the audience.

This project encompasses several fields, including game design, educational theory, and consumer behaviour. To effectively blend these together, a literature review will identify key points in each of these fields which could be combined to produce an effective educational game. Next, an analysis of the field of digital privacy and information security identifies the material to be included in the game, based on actual and perceived risks to everyday users. These concepts are broken down by simplification and analogy, but retain their accuracy even after being put into game form. Finally, an analysis of the minimum viable product for the educational game is presented along with documentation of the creative process followed.

Literature Review

Overview

In order to create an effective educational game which teaches digital natives about privacy and information security, it is important to understand the both the topic and the demographic. This literature review will analyze who digital natives are and how the name arose, as well as their concerns and competencies in the different fields of digital security. It will also look at the definitions of digital literacy and methods that have been developed to measure an individual or group's level of digital literacy. In the field of educational games, several works will be examined for clarification of how an educational game can most effectively achieve its pedagogical goals.

Digital Natives

The term "digital native" was popularized by Marc Prensky in his 2001 paper "Digital Natives, Digital Immigrants," to describe a generation which saw the world in a fundamentally different way thanks to an early and lifelong exposure to technology. At the time, the Internet had already evolved from bulletin boards and Usenet servers into a web of hypertext and rich media. He argued that society was in the middle of such a fundamental shift that traditional educational methods and subjects were at risk of becoming irrelevant to 21st century students. Instead, he claimed, teachers would need to learn to tailor the same material to a generation expecting instant gratification, random access to materials instead of an orderly sequence, and networking with other students instead of learning quietly at individual desks. In the analogy of native and immigrant, being born into a technological world is assumed to have imbued these students with an innate preference for—and familiarity with—that technology. Prensky even goes as far as to posit that the changes could be neurological, making it impossible for digital native students to learn in the style of 20th-century instruction. On the other hand, if teachers are immigrants to the world of their students, the smartest thing they can do is rely on their students to educate *them* about the way things are done in this new world.

Digital Literacy

When describing the changes in thought processes among digital natives, Prensky (2001) essentially suggests a high level of certain digital literacy traits, as later described and categorized by Eshet-Alkalai in his 2004 paper "Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era". Eshet-Alkalai explains digital literacy as follows: "[M]ore than the mere ability to use software or operate a digital device; [digital literacy] includes a large variety of complex cognitive, motor, sociological, and emotional skills, which users need in order to function effectively in digital environments. (p. 93)" He divides digital literacy into five areas, which each encompass a range of activities, interactions, and thought processes that take place in digital environments: (1) photo-visual literacy; (2) reproduction literacy; (3) information literacy; (4) branching literacy, and (5) socio-emotional literacy. He describes these literacies as follows:

Photo-visual literacy deals with an individual's ability to intuitively associate meanings with visual symbols. This skill is used to navigate user interfaces by interpreting icons and layout, and to absorb information from graphical media like pictograms and charts. People with high photo-visual literacy can more effectively follow the flow of a digital environment's menus and instructions without having to consciously decipher the meaning of these abstract symbols.

Reproduction literacy describes how well a person can convert digital information into new forms, by combining and altering existing information. Doing so requires a sufficient level of synthetic thinking to analyze the existing work or works, and take parts of each to produce something unique. There are a wide range of activities that can be considered "reproduction"—anything from slightly altering a piece of writing to avoid plagiarism claims, to fabricating wholly new scholarship by reading existing works in the field. The common factor is that in assessing an individual's digital literacy, it is important to measure their capacity not just to find and absorb information, but also to create and combine what they find into new forms.

Information literacy refers to an individual's eye for accuracy, quality, and bias in the digital information presented to them. Eshet-Alkalai suggests that an information-literate person thinks critically even about information from authoritative sources, or which others assume to be

of high quality. On the Internet, messages are often targeted to individuals based on politics, racial identity, or other personal characteristics. They can come from anonymous sources, or an entire organization can be a false front to hide a deceptive actor. In such contexts, the ability to discern what can and cannot be trusted is key to finding accurate data.

Branching literacy is a navigational skill. A single page on the Internet can lead to others, which in turn lead onward—the name "World Wide Web" is appropriate. When navigating a folder structure or following a trail of links, somebody with branching literacy can remember the path followed and understand the locations of resources in relation to each other. Complex tasks like planning a vacation can require accessing and comparing information across dozens of sites and documents, and retaining the memory of that structure for days or weeks until planning is complete. Branching literacy is fundamental to navigating the Internet, and is the starting point for learning to find and use its resources effectively.

Socio-emotional literacy touches on the ways social norms manifest in digital spaces. Similar to information literacy, a socially literate person on the Internet can accurately identify the nature of interactions and react appropriately. Examples of errors that might result from a lack of this literacy include divulging personally identifying information on a public forum, falling for a romance or marketplace scam, or inadvertently breaking the rules of an online community. More simply, it reflects a certain level of emotional maturity in the way a person interacts and collaborates with others online.

Eshet (2012) updates the 2004 definitions to add a new category of digital literacy: real-time thinking. This change reflects an increase in the number of perspectives and pieces of information that a user must consider when operating complex computer systems. This form of literacy also comes into play when task-switching between multiple programs or devices. As humans cannot truly multi-task, the ability to rapidly shift focus between different interfaces is a skill in itself. Eshet also notes that digital real-time thinking is closely tied to real-world skills like driving and playing games with fast reaction times, and simulations that improve one have been shown to improve the other as well.

Of the original five categories, Prensky specifically ascribes higher photo-visual and branching literacy to digital natives (2001), though he refers to them by description rather than by name. This is borne out by Eshet-Alkalai's analysis, which found evidence that younger test subjects demonstrated higher skill than adults in both areas (2004). However, Eshet-Alkalai (2004) also notes that older people fared better on tests of information and reproduction literacy, which both require a level of maturity and cognition the younger participants may have lacked. In fact, few of the skills grouped under the umbrella of digital literacy are unique to the Internet—though the older "digital immigrant" generation may have grown up without the same exposure to computers, they have more experience with the nuances of human interaction. To a great extent, people online are still very much just people.

Van Dijk and Hacker (2003) also divide the realm of digital literacy into discrete categories, referring to *instrumental*, *informational*, and *strategic* skills. Each corresponds roughly to one or more of Eshet-Alkalai's categories. Instrumental skill—the ability to perform desired tasks with a digital system—requires photo-visual literacy to navigate user interfaces, branching literacy to keep track of digital paths available to traverse, and information literacy to critically evaluate the results obtained. Informational skill is very similar to what Eshet-Alkalai calls information literacy. Strategic skill is related to socio-emotional literacy; van Dijk and Hacker describe it as "the ability to use digital means too [sic] improve one's position in society" (2003, p. 324).

Assessment of Digital Literacy

The apparent advantage of van Dijk and Hacker's (2003) simpler model of digital skill lies in the ease of developing assessments. The three categories of instrumental, informational, and strategic skills correspond more directly with tasks that can be tested and measured, while Eshet-Alkalai's analysis is more precise but also more theoretical. Put simply, dividing digital literacy into five categories requires separate testing methodologies for each type of literacy, even though in many cases the distinctions are less important. For example, Zimic (2010) found that the framework of digital skills developed by van Dijk and Hacker corresponded more closely to questions commonly asked in a specific questionnaire directed to Swedish Internet and

computer users, and therefore chose to use that framework in her analysis. Colloquial definitions of digital literacy ("tech-savviness") often rely on displays of confidence, speed, and familiarity with common computer tasks and issues. These are instrumental skills, but do not directly demonstrate informational or strategic skills. To fill in the gaps, several assessment methods have been developed based on definitions of digital literacy like those proposed by Eshet-Alkalai (2004) and van Dijk and Hacker (2003).

In a study of university students in New Zealand, Sherry and Fielden (2005) developed a self-report survey which asked respondents to rate themselves using a five-point Likert scale on questions which reflected their attitude toward computers, as well as their technical ability. Responses were grouped by age into three categories: under 21, 21 to 25, and over 25. Based on a common definition of a millennial as being born between 1981 and 1996 (Dimock, 2019), only the youngest two age categories in the New Zealand study would include millennials, providing an interesting window into the generational gap between the oldest millennials and the youngest Gen Xers who preceded them into the educational system. The study found that under-21s were more likely to be self-taught when it came to computer use, but also more confident in their instrumental skills and overall level of knowledge. A plurality of these younger respondents chose "comfortable/fairly confident" in response to the question about computer knowledge. Older respondents were more likely to choose just "OK" as their answer, and slightly more inclined to see computers as "difficult to learn" (Sherry & Fielden, p. 494-495). However, when asked ten multiple choice questions ranging from beginner to expert levels of knowledge about each of four commonly used programs, the under-21 age group only had an advantage in Microsoft Word. Scores in the other programs were not statistically significant enough ($p < .05$) to demonstrate a relationship between age and competence. A weak positive relationship did exist between confidence (self-assessment) and ultimate score on the practical questions, but in general Sherry and Fielden concluded that millennials exhibited more confidence than competence.

Calvani et al. (2012) conducted a similar study of Italian secondary school students in 2009-2010 ($n = 1056$), comprising the younger end of the millennial generation. Prior to the survey, the researchers developed an assessment called the Instantaneous Digital Competence

Assessment (iDCA)[1]. The test was written with 87 questions, which were narrowed down over several iterations to choose the most significant 35 questions. Calvani et al. set up this study in order to answer the question discussed earlier: "Does digital literacy amongst younger generations consist only of technical-practical knowledge and skills or does it also include a conceptual understanding of technology, socio-relational knowledge related to the web and high-order cognitive skills which could be involved in their use? (p. 801)" To that end, questions fell into three major dimensions similar to those identified by van Dijk and Hacker (2003)—in this case called "technological", "cognitive", and "ethical" (Calvani et al., 2012, p. 799). They were further narrowed down into specific areas of knowledge, such as visual literacy, troubleshooting, and understanding technological concepts; as well as higher-order cognitive skills like information research and organizing visual data. The results of the survey revealed significant gaps in students' knowledge. When asked basic questions, like identifying items on menu bars or troubleshooting non-functional audio, students answered successfully at a rate of 80-90%. However, when faced with more conceptual questions, such as explaining the potential causes of slow Internet surfing or the use of Boolean operators in a search, the success rate dropped to 45-60% (p. 802). This indicates a high level of instrumental skill, but shortcomings in informational and strategic skills, caused by a lack of understanding of the underlying technological principles. Low scores were found to be correlated strongly with the socio-economic status of the respondents, as well as access to computers in the home, but those factors alone are insufficient to explain the findings. A reasonable conclusion is that students at the ages surveyed lack the higher-order cognitive skills to form appropriate mental models which can encompass their digital environments.

Around the same time frame, the iDCA was translated to Chinese and administered on paper to ninth-grade students in Ningbo, China (Li & Ranieri, 2010). While the Chinese students scored slightly lower than the participants in the Italian study (mean score of 59.69% vs. 62.6%),

[1] The "instantaneous" version of the test consists of only multiple-choice questions, and can be administered online. A "situated" version also exists, which requires setting up an unfamiliar user interface and assessing the student as they learn to operate it (Li & Ranieri, 2010, p. 1033).

several socio-economic factors were identified to explain the difference, including different levels of computer access and teacher preparedness. The results of this second study validate those of the first, and show that the "digital divide" between members of the same educational cohort is linked to early exposure to computers at home and at school. However, the majority of students *do* have daily access to those resources, leading Li and Ranieri to suggest the issue might lie in their thought process and cognitive abilities, and that students may not be as technologically capable as generally assumed (p. 1039).

Teo (2013) describes a tool similar to the iDCA, called the Digital Natives Assessment Scale (DNAS). Like the iDCA, it takes the form of a self-report questionnaire with 35 questions. The topics and questions on the DNAS were determined through an informal group session with participants aged 20 to 35, and include four sections: a) comfort with technology; b) ability to multitask; c) reliance on graphics for communication; d) need for instant gratification and reward (p. 8). These areas of assessment line up closely with both Eshet-Alkalai (2004) and van Dijk and Hacker (2003). While Teo is mainly concerned with statistically validating the assessment for use in school environments, and does not discuss a specific case study where it was implemented, it is helpful to see that other forms of assessment under development take a similar form to those previously discussed (Sherry & Fielden, 2005; Calvani et al., 2012; Li & Ranieri, 2010).

Millennials and Digital Security

This paper describes the creation of an educational game targeted towards millennials and other digital natives who are concerned about online privacy and security. To determine the feasibility of the topic, there are two research questions worth asking. First, is this demographic concerned about these issues? Increased levels of concern indicate an opportunity for relevant educational resources, whereas lower levels of concern mean more explanation is necessary to bring attention to the issue. Second, are digital natives significantly affected by data breaches, identity theft, and other malicious actions? The more commonly these crimes occur, the greater the potential impact of digital literacy education.

millennials are commonly perceived as less concerned about security, desensitized to sharing personal information online by years of using social media. Pereira et al. (2017) question this idea, based on survey results from 1000 American internet users. The data show that millennials do exhibit lower levels of concern across the four categories[2] surveyed, but without a statistically significant increase in social media usage, it is equally likely that this lack of concern is because millennials are simply at a younger life stage to baby boomers and Generation X. They typically hold a lower socioeconomic status and have less medical history, and therefore have less to lose. In support of this possibility, Pereira et al. note that when divided into "younger millennials" (18-27 years old) and "older millennials" (28-35 years old), older millennials were actually more concerned overall than Generation X, despite using social media and health wearables approximately the same amount as the younger demographic.

Data from the United States show that whatever their level of concern, millennials are not immune to identity theft. This category of crime includes new accounts fraudulently opened in an individual's name, unauthorized charges to existing accounts, and "instrumental" fraud, where the person's identity is used to obtain healthcare, employment, or other services. Burnes et al. (2020) report that when broken down by age, millennials do experience these crimes at a rate lower than Generation X, baby boomers, and the Silent Generation—older people are targeted about 25% more often than millennials. However, several factors influence those rates, including the typically lower socio-economic status of millennials when compared to older generations, and identity thieves' preference for stealing married couples' identities for instrumental purposes, where millennials are less likely to be married or partnered. It is therefore not possible to conclude that millennials' lack of concern is justified, especially given that they still make up almost 24% of identity theft victims.

Identity theft is strongly correlated with data breaches—those who report identity theft are up to eight times more likely to have had their data exposed in a breach—so it is possible (to

[2] Privacy of medical information, security of medical information, privacy of online information, security of online information. Pereira et al. (2017) define privacy as a state where only a limited number of people have access to the information, and security as the system of controls which maintain that state.

a certain extent) to use rates of identity theft as a useful stand-in for a demographic's success at protecting its online information (Burnes et al., 2020). Echeverría et al. (2020) analyzed Ecuadorian millennials' digital protection behaviours through a questionnaire (n=103), and found that 24% had experienced fraudulent credit card charges, a further 51% reported receiving a notification that their data had been compromised, and 33% had experienced unauthorized access to their email account. Despite these results, 69% said they used less complicated passwords to make them easier to remember, and another 69% indicated they had not installed any application on their mobile device to increase its security. Jiang et al. (2016) also reported problems with millennials' protection behaviours. In a series of intergenerational focus groups (n=116), all demographics—including millennials—admitted to common bad habits like password reuse, delaying security updates, and neglecting security for the sake of convenience. Although millennials were more likely to research security issues themselves, and to use a password manager, Jiang et al. concluded that "online safety training is needed for all three generations […] to become proficient in protecting themselves online[.] (2016, p. 10)"

The above works deal primarily with security, as opposed to privacy. For example, a consumer webmail account (e.g. Gmail, Hotmail, Yahoo, etc.) is *secure* in the sense that parties not authorized by the user cannot access the account unless a breach occurs. However, the data stored in these accounts is not strictly *private*, since one of the parties in the transaction—the service provider—can unilaterally scan emails to better target advertisements and deliver helpful notifications about travel arrangements. Google stopped this practice in 2017 (Greene, 2017), but other providers like AOL and Yahoo (both owned by the same Verizon Media subsidiary, Oath, since 2018) continue to do so (Handley, 2018).

To demonstrate millennials' level of concern for privacy more directly, one study of college students in the United States found that consumers' perception of a website's privacy commitment significantly affects their e-commerce behaviour. The customers were more likely to purchase items from stores they trusted, and that trust came from multiple sources, including word of mouth, industry self-regulation, and the site's privacy policy (Wang & Herrando, 2019). Mendes (2018) compares the level of privacy concern reported by millennials with their rates of adoption of Internet of Things (IoT) devices, and finds a small but significant negative

correlation, indicating that those with more concern were less likely to use these devices. Consumers want more than the lowest price possible—they want to know that the data collected when making a purchase or setting up a smart home device will not be shared without their consent, whether intentionally or inadvertently through breaches caused by security flaws. The high rate of identity theft victimization among millennials, in combination with their concern for privacy despite exhibiting poor digital security behaviours, indicates a need for educational materials to address these gaps.

Educational Games

As part of his focus on adapting teaching methods to meet the needs of digital natives, Prensky (2001) touches on educational games. Video games, he argues, are already a "familiar idiom" (p. 4) to members of the new generation, and are therefore his preference for adapting traditional material to their language. He describes a project called *The Monkey Wrench Conspiracy,* a game in the style of Doom or Quake[3] which was designed to teach engineers in their 20s and 30s to use a new computer-aided design (CAD) program. Prensky does not present statistics regarding the outcome of the project, but he notes that while it took twice as long to develop a game in this way (due to the shift in thinking required to translate traditional academic techniques to a video game), *The Monkey Wrench Conspiracy* was "phenomenally successful" (p. 5) at getting young engineers interested in learning to use the CAD program, eventually attaining a distribution of over 1 million copies.

Prensky (2001) identifies three specific design choices as having led to positive educational outcomes for his game: avoiding linear progression, increasing the speed and urgency of the game, and removing written material with an academic tone. While these elements are relevant to the project being discussed in this paper, it is not enough to copy Prensky's approach wholesale. In the case of Prensky's CAD instruction game, the audience was composed of technologically-savvy engineers, who had chosen to play the game in hopes of

[3] Two popular first-person shooters released in 1993 and 1996, respectively.

learning a new professional tool, and who presumably had prior experience with other CAD programs. Therefore, it was appropriate to give the players free rein over the order in which they accessed the material, and to increase the pace when necessary to prevent boredom. That may not be true to the same extent when a game is targeted at novices without a strong grasp of the subject being presented, as in the case of the game this paper discusses.

Sauvé et al. (2010) identify six core elements common to educational games: 1) one or more players; 2) conflict; 3) rules; 4) a purpose predetermined by the game; 5) artificial character; and 6) educational character (p. 3). The first five define a game, and the sixth—educational character—describes the underlying pedagogical motivation behind an educational game, without which it would be purely an entertainment product. To develop the educational character of a game, Moreno-Ger et al. (2008) discuss several pedagogical requirements, whether the game is developed from scratch or built on an existing game or platform. Their criteria are a) integration with online education; b) adaptation; and c) assessment. They envision a game integrated with an online learning management system (LMS), capable of connecting students with teachers when they need assistance, as well as adapting on the fly to students' skill levels and learning progression. By building a game as a finite state machine[4] which transitions based on student actions, a developer can ensure that educational character is central to the game's architecture, allowing it to be used as an effective teaching tool while striking the necessary balance between entertainment and education.

Chandross and DeCourcy (2018) also examine the design of serious educational games (SEGs), and note two other pedagogical criteria: achievement and player representation. They note that the most effective form of assessment is continuous and non-punitive, and recognition of player success in the form of digital badges or awards has been shown to increase skill retention. Avatars also create a more powerful motivation in players who can see themselves represented in the game. Emotional engagement is key to self-motivation and self-efficacy,

[4] A *finite state machine*, in computer science terminology, describes a system composed of several finite states (of which only one can be active at a time) which uses logical rules to transition between states. Using these states, the behaviour of the system can be predicted at any point in time (Moreno-Ger et al., 2008).

which in turn influence educational outcomes; by presenting the player with a customizable image of themselves in the game world, they engage more strongly with social situations in-game and see themselves as more competent overall.

Methodology

An informal assessment with a small sample size (n=8) was first used to validate the level of concern the surveyed millennials felt for digital privacy and security issues. Questions were also added to gauge the participants' overall level of technical knowledge, self-perceived competence, and digital security behaviours. In total, the assessment consisted of four sections: **1)** an initial request for information including name, age, and perceived level of knowledge of digital privacy and security on a 10-point Likert scale; **2)** six questions about the respondent's level of concern both in general, and in five specific scenarios, on a 5-point Likert scale; **3)** five questions corresponding to each of the five scenarios in Section 2, asking how likely the respondent was to perform a key digital security behaviour to prevent that scenario from occurring on a 5-point Likert scale; and **4)** a set of multiple-choice technical questions to gauge the respondent's actual level of knowledge in relation to their self-assigned score. Finally, after completing the initial four sections, the participants were asked to again rate their level of digital security knowledge on a 10-point Likert scale. A full list of the questions can be found in Appendix 1.

For the knowledge questions in Section 4, participants were asked to identify which technology is used to secure data in transit from unauthorized access ("encryption"). Later questions were more open-ended, asking the participant to identify which of four parties listed would be able to see certain data in each scenario. For example, Question 3 reads as follows: "When you use a search engine from your computer, who can theoretically see the question you type in? Assume your traffic with the search engine is not using HTTPS[5] for security." The options given are "The company which makes your Internet browser," "The search engine

[5] HTTPS, or "Hypertext Transport Protocol Secure" is an extension of the Hypertext Transfer Protocol underpinning the Internet. Under HTTPS, all traffic between a client and a server (for example, a user and a website) is encrypted using Transport Layer Security. This encryption is almost entirely transparent to the end-user, and ensures that traffic cannot be read by any party other than the intended recipient, even the Internet Service Provider (ISP) which is handling the traffic. However, since the Domain Name Server (DNS) queries which resolve human-readable domain names like "google.com" into machine-readable IP addresses are usually *not* encrypted, it is generally accepted that an ISP will be able to determine the origin and destination, but not the contents, of a given HTTPS-secured session.

company," Your Internet service provider," and "Any application installed on your computer." Due to the open-ended nature of the questions asked in Section 4, multiple answers could be valid depending on variables not specified. In the question asked above, whether an installed application can access network traffic depends on what programs, drivers, and services are already installed on the computer, or whether the user chooses to grant administrative privileges to the program. This was an acknowledged constraint of the online questionnaire, rather than a one-on-one interview. To account for this variability, a marking process was applied to the assessments received. If the respondent identified 3 out of 4 possible answers correctly, the question was marked as "correct" overall. However, if one of the options chosen was not possible from a purely technical perspective (for example, an Internet Service Provider being able to read HTTPS-protected content[5]), this was interpreted as a lack of understanding rather than a difference in assumptions, and the response was marked as "incorrect".

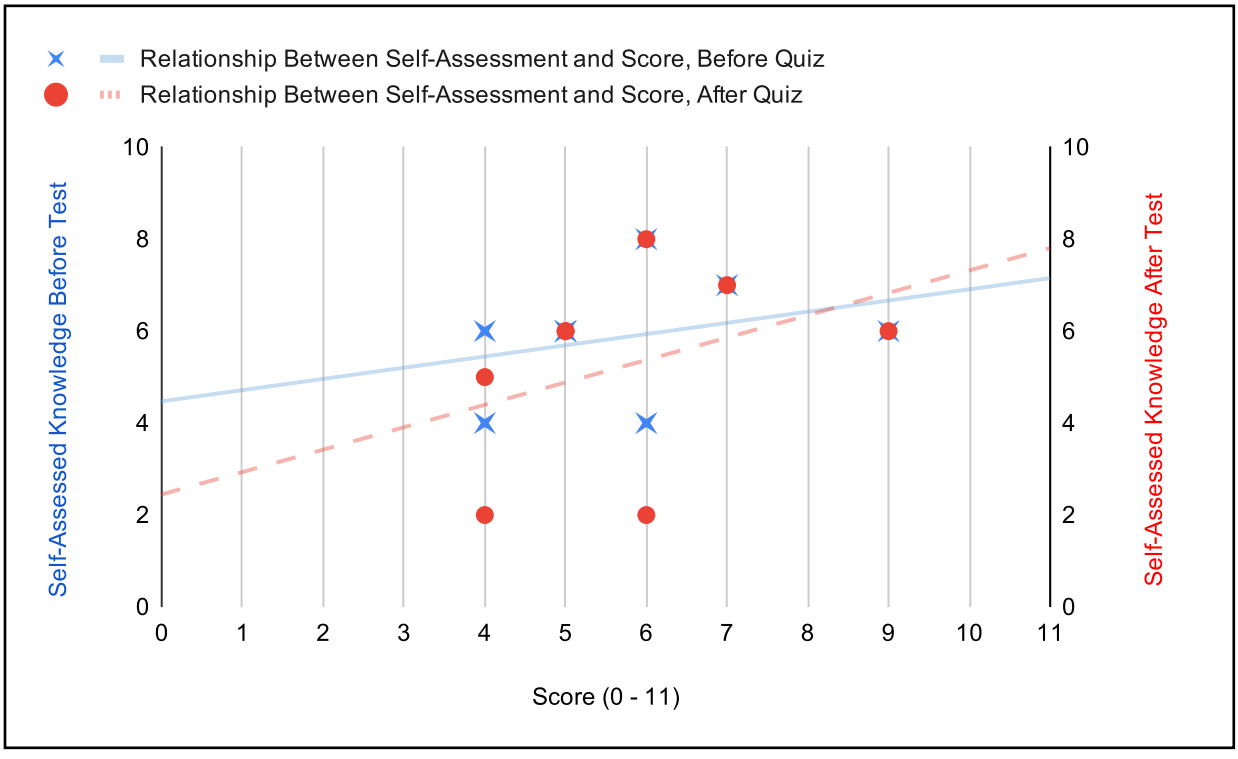

Figure 1: *How did participants' self-assessment scores correspond to test scores, before (left) and after (right) self-adjustment?*

The results of the initial survey validated the literature reviewed above and provided further guidance for specific digital security topics that would be effective candidates for the game being proposed. The mean score was 6 out of a possible 11 points (54.5%), which tracked

closely with the mean of the participants' self-reported digital security knowledge (58.8%). After completing the assessment, 3 out of 8 participants (37.5%) revised their self-assessed knowledge downwards. Figure 1 shows the correlation between self-assessed knowledge both before (left axis, blue solid line) and after (right axis, red dashed line) completing the assessment. The initial trend was slightly positive, indicating that higher self-assessment was weakly correlated with higher scores. However, the increase in positive trend after several participants revised their self-assessed knowledge score suggests that the revised, lower self-assessment scores were more accurate predictors of eventual test scores.

The participants in the survey were asked about their general level of concern, as well as specific scenarios (e.g. having data stolen while using public Wi-Fi) and digital security behaviours that correspond to those scenarios (e.g. confirming that all websites accessed are using HTTPS). Results were consistent, with averages for general concern, each specific concern, and security behaviour adherence identical within the margin of error (72.5%, 75.7%, and 71.5% respectively). These results are similar to those obtained by Echeverria et al. (2020), indicating a base level of self-protection, but with notable deficiencies. Evaluation of the data did find differences between stated concerns and security behaviours in specific scenarios. Both concern and behaviour were evaluated on a 5-point Likert scale, and in three of the five scenarios, participants reported their level of concern as higher than their likelihood to take precautions against it. Most notably, the scenario which raised the most concern among participants ("Inadvertently downloading a virus or other malicious software.") was rated an average 4.5/5, yet when asked about the corresponding digital security behaviour ("Update virus definitions, if using anti-virus software, and run a security scan of your device.")[6], the likelihood of taking the necessary precautions was only 3.75/5.

Although limited by a small sample size and relative lack of rigor in the survey methodology, the assessment suggests that millennials have a generally accurate idea of their

[6] Another example of a question that could have been asked is whether participants *had* anti-virus software installed on their device. The wording indicated was chosen to require active action on the participants' part, and to eliminate any confusion about whether an operating system's native protection systems are considered anti-virus software.

own level of knowledge. It identifies several areas of investigation where the respondents exhibited a lack of basic knowledge, specifically around the purpose of security tools like HTTPS and virtual private networks (VPNs). Finally, the results also indicate that millennials do exhibit concern for common digital security scenarios but may take fewer precautions than advisable.

The game this paper focuses on, titled “The Scoop”, was developed in parallel with the assessment discussed above. It was built using the Unity game engine, which is free for personal and educational use, and offers modules which allow a developer to build a project for multiple platforms simultaneously. In this case, the Web Graphics Library (WebGL) platform was chosen for the prototype and final build stages, to allow the project to run in any supported Web browser, primarily Google Chrome. Within Unity, the programming for the game was done in the C# language, and Unity’s native Scriptable Objects were used to allow drag-and-drop programming of game dialogue, levels, and overall sequence. Moreno-Ger et al. (2008) discuss the use of eXtensible Markup Language (XML) in the context of an e-adventure educational game, but the structure of XML is suited more to a text-based game integrated closely with a Learning Management System (LMS), as opposed to a standalone game built with conventional graphics and animation. In addition, the JavaScript scripting language for Web browsers was considered for the programming and graphics, specifically through a third-party game engine library for JavaScript. This was not implemented for several reasons, primarily my familiarity with Unity, as well as the lower level of community support for JavaScript game engines like melonJS (2020) and Phaser (2020). Throughout the creative process, Unity’s foundation of solid support for both two-dimensional (2D) and three-dimensional (3D) graphics, as well as audio and game logic, enabled the creation of not just a single game, but a platform capable of supporting games from different genres, focusing on different educational topics, and even reconfiguring dialogue, tutorials, graphics, and the game sequence without any programming knowledge.

Implementation

Based on the results of the assessment, as well as a review of the relevant literature, the specific roles of HTTPS[5] and virtual private network (VPN) technology were identified as the two areas of educational content to be included in the minimum viable product (MVP). The board game genre was chosen due to its simplicity, its familiarity even to those unaccustomed to video games, and the ease of modularity compared to a fully realized 3D game. Moreno-Ger et al. (2008) describe the process of first choosing a genre, then a topic, and finally developing a curriculum of educational items to be inserted into a game of that genre. Following this process allowed for considering the constraints of the chosen genre from the beginning of the development cycle, as opposed to encountering frustration when trying to force existing educational content into a type of game not suited for it.

In this case, a board-game with a top-down view[7] is best suited for moving pieces in two dimensions around a fixed board. Gros (2007) describes a taxonomy of seven major game genres, with the closest match for The Scoop being an adventure game— "the player solves a number of tests in order to progress through a virtual world" (p. 26). The pieces and board squares can be representations of different elements in the infrastructure of the Internet, such as data packets, devices attempting to "sniff" or spy on user data, or possible destinations. With those constraints in mind, the curriculum was designed to convey the main points through the gameplay itself, with finer details included in the tutorial text displayed to the user at the beginning of certain levels or when taking certain actions for the first time. The core gameplay loop is as follows:

1. The player begins the game and creates an avatar using provided skin tone, hair style, and face shape options.

[7] A 2D top-down view was chosen over a 3D isometric view to reduce the complexity of the camera controller programming, and to simplify the appearance of the game board for new players.

2. Some dialogue takes place between the player and one or more characters, introducing or expanding the story (a rival ice cream company is trying to steal a secret recipe).
3. The player must pass several levels of the game, encountering new items and obstacles. To beat a level, one or more packages must be placed on a two-dimensional board, and moved to an exit square using a combination of forward moves, which are unlimited, and a predetermined number of arrow items that can move packages in other directions.
4. After beating a certain number of levels (one to four, depending on the specific stage), the player returns to the town and encounters another dialogue scene.
5. The cycle from #2-4 continues until all levels have been passed.
6. The player is returned to the main menu, where they can either continue their previous game or start a new game from the avatar creation screen.

Although intended as an educational game, The Scoop is oriented towards the "fun" side of the fun/educational dichotomy identified by Prensky (2001). The levels are fairly challenging from a puzzle perspective; while the additional challenge does not directly illustrate a particular educational point, it serves to engage the player which in turn increases their immersion in the game and the likelihood of absorbing the educational material through gameplay and tutorial text.

For the HTTPS section, the main point to convey was the comparison of HTTPS-secured traffic with a "locked box", where the box itself is visible to others but the contents cannot be discerned. In-game, this took the form of a lock item which could be applied to a package. On certain levels, trap squares can catch the packages as they move through, forcing the user to restart the level until they discover that applying a lock to the package protects it from the trap. Several smaller details are communicated through other means. The first time a player applies a lock, an information box appears with additional text explaining that HTTPS uses encryption to conceal the contents of an Internet packet, but not its source or destination. In several dialogue scenes, the player's avatar discusses the advantages and disadvantages of locks in the game, indirectly explaining the role of HTTPS in Internet security.

For the VPN section, the main point being conveyed was that a VPN is like a tunnel, where traffic is visible entering and leaving, but while inside the tunnel its origin and destination cannot be easily determined. Later in the game, the player is given access to keys which unlock special "gate" squares. When a gate square is unlocked, a predetermined series of extra squares appears around the perimeter of the board, opening new possibilities for movement and potentially allowing the player to reach an exit which was previously inaccessibly. As with HTTPS, the main point is communicated through the gameplay, while smaller details are left to tutorial text and expository dialogue. When a player clicks on the key item to open a VPN gate for the first time, a text pop-up reminds them to ensure their package will be secure where the tunnel terminates. The real-life analogy in this case is the vulnerability a user's traffic is exposed to when it exits the protected VPN tunnel. An unscrupulous service provider might log the traffic a user sends and receives, or even monitor any unencrypted (non-HTTPS) traffic sent over the VPN. The pop-up provides the user with a list of red flags and questions that can help identify a secure VPN service provider. In the dialogue sections of the game, the main villain who is attempting to steal the secret ice cream recipe from the player's character refers to the fact that no matter how long the player remains underground, they must surface eventually. Again, the main educational objective is conveyed through gameplay, while finer details and additional information are given in tutorials and dialogue.

Moreno-Ger et al. (2008) discuss potential starting points for programming an educational game, including 1) a purely educational approach based on displaying multimedia content ("edutainment"), 2) repurposing an existing game for a specific educational purpose, and 3) a middle ground consisting of video games specifically built to convey educational content. Several challenges are identified with the third approach, although Moreno-Ger et al. state that striking a balance between fun and education is the key to a successful educational game. One challenge is the game design skill necessary to make something "fun", which is further increased when the game must convey information the player might not find inherently interesting. Additionally, designing a game from scratch carries additional development time and cost; while cost was not directly a factor in this project, development time certainly increased as a result of choosing to start with no pre-written framework or platform other than the Unity engine's basic

tools. However, retaining control over the game's code and assets greatly simplified implementation and customization of necessary features like character art, piece behaviour, and the flow of the game.

When approaching the programming of the game itself, the three key considerations mentioned earlier were simplicity, modularity, and familiarity. Simplicity was defined as limiting the number of choices available to the player at any point in time. To achieve this, the game was built with a single mechanic (moving pieces on a board), and items were gradually introduced one at a time to expand on the base mechanic. In the following levels, a new concept could be combined with others to produce emergent challenges the player could discover for themselves—for example, in one level, the player is shown that a trap pushes a package away when it intercepts it; in the next level the player must use this technique to complete the objective. This initial simplicity and gradually increasing complexity are used to engage the player and indirectly increase their exposure to the educational content in the game.

Modularity refers to the ability of the game elements to be altered, removed, or recombined without changing the underlying programming. The Unity game engine provides a class of object referred to as a *scriptable object* (or ScriptableObject), which is a reusable component capable of holding a predetermined set of data and providing that data to the game as it runs. The scriptable objects can be organized in a folder hierarchy and dragged-and-dropped into other game objects, which then use the data held in the objects to run the game. Scriptable objects can even hold other scriptable objects, enabling nested layers of *encapsulation*[8]. Encapsulation is a term in computer science referring to the containment of simpler data types inside more complex ones. For example, in The Scoop, the core game structure is composed of

[8] Encapsulation has multiple definitions in the context of computer science. When discussing object-oriented programming, encapsulation is the practice of creating an object which holds both data and methods for manipulating that data, and which hides its internal state from external access. However, the context used here is more like computer networking, where a hierarchy of data types exist, corresponding to the OSI seven-layer network model (International Telecommunications Union, 1994). The idea is to encapsulate the entirety of a higher-level data packet (including its metadata) within the data payload of a lower-level packet. This eliminates the need for lower-level transport layers to "understand" the higher ones, increases interoperability, and reduces the apparent complexity at any point in the system.

"acts", which each contain an optional "conversation" and zero or more "levels". A "conversation" is in turn composed of multiple "dialogue blocks", which each indicate the character (also a scriptable object), camera location, and lines to display for a given section of dialogue (Figure 2). This modularity allows an educator or developer to, for example, alter a line of spoken text, to control the items given to a player, or even change the layout of a level's board entirely, without having to edit code or recompile the game.

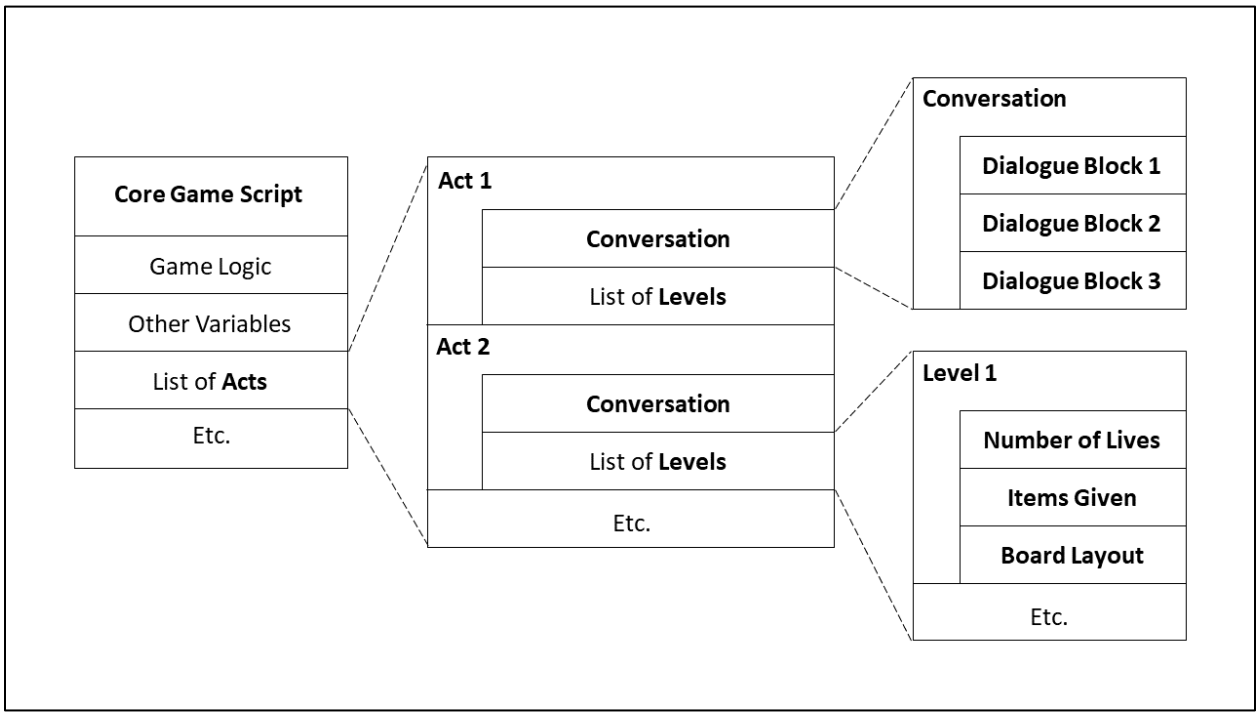

Figure 2: *A diagram showing the encapsulation of the game's data types within each other. Blocks toward the right represent more granular elements of the game.*

Familiarity was a key design goal because it allows even players new to video games to be comfortable playing The Scoop. In particular, the choice of the board game genre draws comparison with classic games like checkers or chess, which are widely recognized. Another design decision was always to keep the entire board visible, rather than representing a larger space with smaller "sub-maps" which the player could transition between. With a few changes, the gameplay element of The Scoop could even be represented on a physical checkerboard with very little loss of fidelity. While the game does provide both video and text-based tutorials, the intent is to keep the players engaged who would be most likely to abandon play after early failures.

When it comes to player demographics, video games show significant differences between male and female players. Male video game players are more likely to play alone than female players (Ohannessian, 2018), and previous studies of millennials have shown that when surveying gamers who play daily for at least half an hour, 65% are male while only 35% are female. However, 94% of the female respondents said they played regularly, demonstrating that although female video game players are less likely to play daily than males, the demographic does exist and can be marketed to (Lenhart et al., 2008). Male players are more likely to seek and enjoy violence in video games than female players, which may be tied to female players' generally greater level of empathy and tendency to see the opponent as an individual, and therefore enjoy violence less (Hartmann et al., 2015). The decision was therefore made to avoid violence, both to prevent alienating any players who prefer to play games without violence and to ensure the game is appropriate for all educational environments, including players potentially younger than those envisioned by the scope of this paper.

Avatar creation was an important feature added to the game to further increase player engagement and encourage players to see themselves as having increased digital literacy. Chandross & DeCourcy (2018) discuss findings which show an in-game avatar can greatly motivate players, though the impact on actual learning outcomes are still undetermined. In the case of The Scoop, player motivation is one of the key challenges of marketing the game, as millennials are generally finishing with post-secondary education and entering graduate education or full-time employment. Players therefore might be exposed to the game through word of mouth or encountering it online, rather than a formal program of study, and feel no obligation to play through the entire game if it does not provide enough motivation to do so. As discussed above, the WebGL platform was chosen to increase accessibility by removing barriers such as file downloads and security concerns. For similar reasons of player engagement and retention, the avatar creation screen is the first interface shown to the player after beginning a new game, and the avatar they create is saved in the browser's storage so it reappears even after reloading or navigating away from the page.

Evaluation

While no follow-up assessment was conducted with the original survey participants to validate the transfer and retention of educational information from the game, The Scoop serves as a theoretical demonstration of how such a game can be implemented using low-cost tools and conventional programming techniques. In particular, the inclusion of widely varied methods of instruction—gameplay, text, and pre-recorded video—leaves several avenues open for further research into the efficacy of each method.

Several decisions in the development of the game are also acknowledged to have limited the educational potential of the final product, and instead served as creative exercises for my own benefit. These can serve as counterexamples of choices which can hamper the development of a creative project if not made carefully. Specifically, most of the assets used for characters, menus, backgrounds, and game pieces were hand-drawn in a pixel art program, specifically for The Scoop. This represents a significant investment of time which could otherwise have been used to build more educational content or new gameplay features. Toward the end of development, the decision was made to use license-free stock assets for the user interface and some of the game pieces, and this enabled more resources to be focused on finding game bugs and polishing the educational aspects of The Scoop. While a unique, hand-drawn art style greatly contributes to the final product, it is worth considering the potential impact to development cost and time when weighing these factors.

Similarly, the decision to teach primarily through analogy resulted in the creation of an entirely unique style of game. Moreno-Ger et al. (2008) discuss the relationship of genre and curriculum and note that choosing the genre first avoids some frustration around having to fit educational content into an unsuited type of game. This is true to an extent, but when the game is being built from scratch, there are also opportunities to revisit the design of the game itself if opportunities are later identified to include important educational concepts. For example, the VPN tunnels seen in later levels were not originally included in the game but were added after survey respondents exhibited some uncertainty about the principal functions and drawbacks of VPNs. However, as Moreno-Ger et al. note, this bespoke approach to educational game

development carries significant increases to development time, cost, or both. A more cost-effective game might have presented players with pages of text, or simple animations, to illustrate the key points, then presented a short quiz which gave points or similar rewards to reflect correct answers. When developing this type of game, more time could be spent refining the dialogue and art, while potentially achieving similar educational outcomes, at the expense of some level of fun.

It is also important to look at The Scoop through the analytical lenses discussed earlier. Prensky (2001) noted some success with an educational game project where he took care to add non-linear progression, increase the pace to keep players interested, and remove any text with an academic tone. The Scoop fulfils two of those criteria—increased pace and non-academic tone—but does not present the player with any non-linear story options. As noted above, Prensky's game was targeted at experienced users of a particular type of software (CAD), and it was assumed that the learning curve would differ between players. In this case, the potential players surveyed displayed similar levels of knowledge, and a linear progression is likely justified in order to avoid instances of a player "skipping ahead" and lacking the base knowledge to beat the level.

Sauvé et al. (2010) discuss a more formalized set of criteria to characterize an educational game. The Scoop fulfils these as well: 1) one or more players; 2) conflict; 3) rules; 4) a purpose predetermined by the game; 5) artificial character; and 6) educational character. The 6th criterion, educational character, is most relevant for discussion here. Sauvé et al. identify a distinction between *educational* and *pedagogical* games; in the former, the educational purpose is hidden from the player and the game is more centered around pleasure. In the latter, the experience is centered around learning, and the game directly appeals to the player's desire to learn. Based on these criteria, the game described in this project would fall into the first category, that of an educational game, as education is made secondary to the player's level of enjoyment.

The Scoop does lack several key elements of educational games identified by Moreno-Ger et al. (2008), namely assessment, adaptation, and integration. This is explained by the key distinction between *educational* and *pedagogical* games, where Moreno-Ger et al. seem to be

referring to the latter. While a game capable of adapting itself to the player's desires and skill levels would certainly serve a purpose as an educational game, such a system would be better suited for generating accurate assessments of players as a pedagogical tool. From a pure game design perspective, it is not always desirable to have the game match the player's skill level, as part of the enjoyment of playing a video game often comes from being able to greatly increase one's skill level beyond the challenge posed by a specific level. Similarly, The Scoop lacks features related to assessing players and communicating directly with a learning management system (LMS) which would be employed by a school or organization to track training progress. These features could certainly be added, using the same lines of code which currently trigger the pop-up information windows the first time a user takes a certain action or makes a specific mistake, but doing so was not a priority when establishing the minimum viable product.

Chandross & DeCourcy (2018) add one further criterion, player representation. As discussed earlier, adding a player's avatar to the game can increase engagement and improve the player's perception of their own competence. Several features in The Scoop address this goal. Players are invited to create their own avatar when starting the game, including a wide range of skin tones and hairstyles. Later, while progressing through the game, the player avatar is featured prominently in dialogue, and is shown coming up with the core ideas which lead to the story's resolution. In levels, the player avatar is always present onscreen, further drawing the player into the world and making them feel present in the game. Li et al. (2013) discuss the benefits of Player-Avatar Identification (PAI), including a stronger emotional connection to the game, as well as mirroring of the avatar's onscreen behaviour in real life. In the current version of the game, the player's name is not requested, and therefore not incorporated into the dialogue or user interface in any way, partly due to concerns about data collection on the online platform hosting the game; this could be added as another powerful element of player representation in-game.

Conclusions

The original aim of this project was to validate that digital privacy and security is an area where millennials are impacted by a lack of digital literacy and technical knowledge, and to undertake the creation of a game to help address that shortcoming. In that regard, the project has been largely successful. The sources discussed in the review of the relevant literature found a significant level of concern among millennials, especially those in the older half of the generational cohort, for their own digital privacy and security (Pereira et al., 2017). At the same time, Jiang et al. (2016) and Echeverria et al. (2020) identified specific deficiencies in digital security behaviours among millennials, such as reusing passwords—thereby increasing their vulnerability in the event of a corporate data breach—and delaying important security updates on their devices. An informal assessment undertaken as part of this project validated many of the research findings and provided some guidance for potential game topics; once the topics were chosen, a curriculum was developed and incorporated into the chosen genre of game.

As well as building the game itself, this project also aimed to establish guidelines for undertaking the creative and technical development of an educational game and provides both examples and counterexamples of decisions in the development process which can influence the success of a project. These decisions include:

- What platform will the game be built on, and where will it be deployed?
- Will the game be programmed from scratch, built on an existing product, or focus more on text and media with very little gameplay at all?
- What is the right balance of stock assets versus bespoke graphical elements to fit the time and budgetary constraints of the project?
- How can the game incorporate modular elements which allow for later modification or rearrangement without further programming cost or complexity?
- If necessary, how will the game provide assessment to players and integrate with an LMS?

In the case of The Scoop, these questions were answered during the development process, leading to a product which meets the expected standard in some areas (graphical quality,

gameplay) but falls behind in others (amount of educational content). The intention is for this work to lead to the development of more formalized development guidelines which bridge the conversation between creative and technical personnel on a project, ensuring the game or software being created suits the needs of all stakeholders and is completed successfully within the initial budget and timeframe.

Future Works

Based on the guidelines discussed above, this format of game lends itself to several types of expansion. Within the topic chosen—privacy and digital security—there are several areas crucial to a basic understanding that are not covered in The Scoop's MVP. For example, one key aspect of digital security is the establishing of trust between two parties, who may or may not have any method of verifying each other's identities offline. In the initial questionnaire, trust was one of the areas where respondents struggled to answer correctly. Generally, they displayed a tendency to over-trust security symbols, such as the HTTPS padlock in a browser; when asked to describe the benefit of using encryption on an online storefront, seven out of the eight participants incorrectly listed benefits like "you will receive the item you are purchasing" and "Even if the merchant suffers a data breach (is hacked), your personal information is safe." While the areas discussed in The Scoop are valuable, establishing and verifying trust is perhaps just as crucial to maintaining safety online, and a game capable of educating millennials on that topic could carry similar benefits.

There are several areas of the current game which could be expanded to add additional functionality. Likely the most important from an educational perspective is adding integration with a learning management system (LMS) to collect analytics, assess players' performance, and award digital badges and achievements. An LMS would allow the game to start off with an existing idea of who the player was, their level of success on previous games or assessments, and even adjust the level of challenge in the gameplay accordingly. Instead of asking users to create an avatar, the game might be able to use a photo and name provided by the LMS. However, as discussed earlier, The Scoop is primarily an educational game as opposed to a pedagogical tool. To better fit a specific course or educational objective, the game would need to be redesigned to increase the density of educational content, and to surface that content in more obvious ways than passive absorption and skippable tutorials.

During the initial phases of the project, other areas of technology were identified as potential candidates for additional games in the same vein, including extended reality[9], cloud computing and data storage, computer networking, and artificial intelligence. Each of these could form the basis of a project with similar scale and style. For example, a computer networking game might focus on the transport of data between two devices, with the benefits including a better understanding of how to set up and maintain a home network environment and diagnose some user-repairable connection issues. Helpful analogies already exist for many networking topics and would integrate well into gameplay mechanics—the Internet could be represented by a series of pipes between buildings, with each building having a unique address (IP address). The issues identified earlier in this paper are not specific to digital privacy and security, with many other areas of millennials' everyday lives affected by a lack of digital literacy and technical knowledge.

Outside of technology altogether, the style of game documented in this work is best suited for perhaps the most challenging type of educational game—one where a complex topic is being taught to a user who may not be fully engaged. A potential customer for such a game might be a government agency or NGO tasked with raising awareness about a global issue. In this scenario, building an educational game—as opposed to a pedagogical one—helps avoid the game becoming laborious, boring, or preachy. A conventional multi-media focused experience might only be suited to hosting on the agency's Web site. However, a game with fun as its central focus can also be distributed through conventional channels such as the Steam video game marketplace, where games are algorithmically promoted to potential customers based on player feedback, further increasing the game's reach without additional marketing expense.

[9] Extended reality refers to the combined field of virtual reality, where users are shown an entirely simulated world through a headset or goggles; and augmented reality, where computer-generated elements are overlaid onto real-world imagery.

Appendix 1: Preliminary Assessment Questions

Format: "Question: Description *(where applicable)*"

Section 1

1. Name: Please enter your preferred name here.
2. Age: Please enter your age
3. Email Address
4. Rate your knowledge of digital privacy and security on a scale of 1 to 10.

Section 2

1. What is your overall level of concern for your personal digital security and privacy? (1 to 5)

   Participants were then asked to rate their level of concern for each of the following scenario, again from 1 to 5:

2. Shopping or logging into online banking, while connected to a public Wi-Fi network.
3. Advertisers collecting information about websites you visit and items you shop for online, then using that data to build a consumer profile of you.
4. Inadvertently downloading a virus or other malicious software.
5. Somebody else accessing your social media or email account, using a password obtained through hacking or a data breach.
6. Data collection in your home through a smart home device.
   Data Collection: e.g. audio, video, location, network info. Smart home device: e.g. Google/Alexa speaker, Nest thermostat, Hue lightbulbs, Blink security camera, Facebook Portal, etc.

Section 3

Participants were asked how likely they were to do each task, from 1 to 5

1. Check that a shopping site is using HTTPS (secure browsing/"padlock") before entering credit card details.

2. Turn on a “Do Not Track” browser setting or extension, use Incognito Mode, or clear cookies regularly.

   *In this context, using Incognito Mode *does not* include using it for the purpose of preventing specific browsing history from appearing on the local computer ("private browsing").*
3. Update virus definitions (if using anti-virus software) and run a security scan of your device.
4. Turn on two-factor authentication (2FA) for online accounts, and use unique, complex passwords (or a dedicated password manager).
5. Read terms and conditions for new smart home devices, turn off any optional monitoring or diagnostics.

Section 4

Multiple choice. Bold answers are “correct”, though as noted above, a grading process was applied to questions with multiple possible interpretations.

1. _____ protects data by hiding it from third parties, using mathematical operations and a secure key.
   a. **Encryption**.
   b. Solid state storage.
   c. A Zip file.
   d. “Hiding” a folder on your computer.
2. HTTPS (secure hypertext transport protocol) encrypts data between _____ and _____.
   a. Your house and your Internet Service Provider (ISP).
   b. Your computer and your Wi-Fi router.
   c. Your computer and the site you’re visiting.
   d. Your ISP and the site you’re visiting.
3. When you use a search engine from your computer, who can theoretically see the question you type in?

   Assume your traffic with the search engine is not using HTTPS for security. Select all that apply.
   a. The company which makes your Internet browser.
   b. The search engine company.

c. Your Internet service provider.

d. Any application installed on your computer.

4. For the question above, if your connection was secured with HTTPS, who would still be able to see your search queries?

   Select all that apply.

   a. The company which makes your Internet browser.

   b. The search engine company.

   c. Your Internet service provider.

   d. Any application installed on your computer.

5. When using HTTPS, what data is still visible to your Internet Service Provider (ISP)?

   Select all that apply.

   a. The names of sites you visit.

   b. The amount of traffic to and from your location.

   c. Your public IP address.

   d. The content of sites you visit.

6. Using strong encryption on an e-commerce (shopping) webpage means:

   Select all that apply.

   a. You will receive the item you are purchasing.

   b. A bank has verified that the merchant stores credit card data securely.

   c. A person on the same network as you cannot intercept your credit card details.

   d. Even if the merchant suffers a data breach (is hacked), your personal information is safe.

7. What is a guaranteed way to verify that an email came from the claimed sender?

   Select all that apply.

   a. Secure padlock in the browser address bar.

      (a photo of the icon is attached to the answer)

   b. The sender mentions a previous email conversation, that only the two of you were part of.

c. Your mail client displays the person's name in the "From" field, and does not flag it as spam.

d. **Directly verifying with the other person via a separate means of communication.**

8. In which of these scenarios can information about your Internet activity still be linked to your advertising profile?

   e.g. Facebook or Google tracking. Select all that apply.

   a. Using Incognito mode.

   b. Using a VPN.

   c. Using a different Web browser.

   d. Using a different computer on the same network.

   e. Using a public computer on a different network, without signing into any accounts.

9. Which of the following types of data can be collected by an advertiser (e.g. Facebook) even while you're not browsing their website?

   a. Names and addresses of sites you visit

   b. Details about items you clicked on or added to a shopping cart

   c. Searches on other websites

   d. Purchases on other websites

   e. Camera and microphone data from your computer

10. If you are using a virtual private network (VPN), your network traffic is:

    Select all that apply.

    a. made to appear as though it came from a different location.

    b. encrypted.

    c. not logged or monitored.

    d. often slowed down.

11. When using a VPN, what data is still visible to your Internet Service Provider

Select all that apply.

a. The names of sites you visit.

b. The amount of Internet traffic to and from your location.

c. **Your public IP address.**

d. The content of sites you visit.

Section 5

1. Rate your knowledge of digital privacy on a scale of 1 to 10.

References

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and Protective Factors of Identity Theft Victimization in the United States. *Preventive Medicine Reports*, *17*, 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Calvani, A., Fini, A., Ranieri, M., & Picci, P. (2012). Are Young Generations in Secondary School Digitally Competent? A Study on Italian Teenagers. *Computers & Education*, *58*(2), 797–807. https://doi.org/10.1016/j.compedu.2011.10.004

Chandross, D., & DeCourcy, E. (2018). Serious Games in Online Learning. *International Journal on Innovations in Online Education*, *2*(3). https://doi.org/10.1615/IntJInnovOnlineEdu.2019029871

Diane Greene. (2017, June 23). As G Suite Gains Traction in The Enterprise, G Suite's Gmail and Consumer Gmail to More Closely Align. *Google Product Updates*. Retrieved from https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

Echeverría, M., Garaycoa, M., Tusev, A., Echeverría, M., Garaycoa, M., & Tusev, A. (2020). Are Ecuadorian Millennials Prepared Against a Cyberattack? *Revista Chakiñan de Ciencias Sociales y Humanidades*, (10), 73–86. https://doi.org/10.37135/chk.002.10.05

Eshet, Y. (2012). Thinking in the Digital Era: A Revised Model for Digital Literacy. In Eli B. Cohen (Ed.), *Issues in Informing Science and Information Technology* (pp. 267-276). Santa Rosa, California: Informing Science Press.

Eshet-Alkalai, Y. (2004). Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *Journal of Educational Multimedia and Hypermedia*, *13*(1), 93–106.

Gros, B. (2007). Digital Games in Education. *Journal of Research on Technology in Education*, *40*(1), 23–38. https://doi.org/10.1080/15391523.2007.10782494

Handley, L. (2018, August 29). Yahoo and AOL are Reportedly Scanning Emails for Data to Sell to Advertisers. *CNBC.* Retrieved from: https://www.cnbc.com/2018/08/29/yahoo-and-aol-are-said-to-scan-emails-for-data-to-sell-to-advertisers.html

Hartmann, T., Möller, I., & Krause, C. (2015). Factors Underlying Male and Female Use of Violent Video Games. *New Media & Society*, *17*(11), 1777–1794. https://doi.org/10.1177/1461444814533067

International Telecommunications Union. *Information technology—Open Systems Interconnection—Basic Reference Model: The basic model.* (1994, July). Retrieved from https://www.itu.int/rec/T-REC-X.200-199407-I/en

Jiang, M., Tsai, H. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational Differences in Online Safety Perceptions, Knowledge, and Practices. *Educational Gerontology*, *42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

Lenhart, A., Kahne, J., Middaugh, E., Macgill, A. R., Evans, C., & Vitak, J. (2008). *Teens, Video Games, and Civics: Teens' Gaming Experiences Are Diverse and Include Significant Social Interaction and Civic Engagement.* Pew Internet & American Life Project. Retrieved from https://eric.ed.gov/?id=ED525058

Li, D. D., Liau, A. K., & Khoo, A. (2013). Player–Avatar Identification in Video Gaming: Concept and Measurement. *Computers in Human Behavior*, *29*(1), 257–263. https://doi.org/10.1016/j.chb.2012.09.002

Li, Y., & Ranieri, M. (2010). Are 'Digital Natives' Really Digitally Competent?—A Study on Chinese Teenagers. *British Journal of Educational Technology*, *41*(6), 1029–1042. https://doi.org/10.1111/j.1467-8535.2009.01053.x

melonJS. (2020). *melonJS*. Retrieved from http://www.melonjs.org/

Mendes, I. F. M. (2018). *Does Online Privacy Matter?: A Comparative Study of Portuguese and German Millennials* (Master's thesis). Retrieved from https://repositorio.ucp.pt/handle/10400.14/25629

Michael Dimock. (2019, January 17). *Defining Generations: Where Millennials End and Generation Z Begins.* Pew Research Centre. Retrieved from https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

Moreno-Ger, P., Burgos, D., Martínez-Ortiz, I., Sierra, J. L., & Fernández-Manjón, B. (2008). Educational Game Design for Online Education. *Computers in Human Behavior*, *24*(6), 2530–2540. https://doi.org/10.1016/j.chb.2008.03.012

Ohannessian, C. M. (2018). Video Game Play and Anxiety During Late Adolescence: The Moderating Effects of Gender and Social Context. *Journal of Affective Disorders*, *226*, 216–219. https://doi.org/10.1016/j.jad.2017.10.009

Pereira, S., Robinson, J. O., Peoples, H. A., Gutierrez, A. M., Majumder, M. A., McGuire, A. L., & Rothstein, M. A. (2017). Do Privacy and Security Regulations Need a Status Update? Perspectives from An Intergenerational Survey. *PLOS ONE*, *12*(9), e0184525. https://doi.org/10.1371/journal.pone.0184525

Phaser—A Fast, Fun and Free Open Source HTML5 Game Framework (2020). Phaser. Retrieved from http://phaser.io

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon*, *9*(5), 15.

Sauvé, L., Lise Renaud, & Kaufman, D. (2010). *Games, Simulations, and Simulation Games for Learning: Definitions and Distinctions*. https://doi.org/10.4018/978-1-61520-731-2.ch001

Sherry, C. A., & Fielden, K. A. (2005). The Millennials: Computer Savvy (Or Not?). *Higher Education in a Changing World: Research and Development in Higher Education. Proceedings of the 2005 HERDSA Annual Conference.*, *28*, 11. Sydney, Australia: HERDSA.

Teo, T. (2013). An Initial Development and Validation of a Digital Natives Assessment Scale (DNAS). *Computers & Education*, *67*, 51–57. https://doi.org/10.1016/j.compedu.2013.02.012

van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. *The Information Society*, *19*(4), 315–326. https://doi.org/10.1080/01972240309487

Wang, Y., & Herrando, C. (2019). Does Privacy Assurance on Social Commerce Sites Matter to Millennials? *International Journal of Information Management*, *44*, 164–177. https://doi.org/10.1016/j.ijinfomgt.2018.10.016

Zimic, S. (2010). *Opening the Box: Exploring the Presumptions About the "Net Generation"* (Licentiate thesis). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-12189