Digital Privacy: Leadership and Policy

DIGITAL PRIVACY: LEADERSHIP AND POLICY

LORAYNE ROBERTSON; BILL MUIRHEAD; JAMES ROBERTSON; LAURIE CORRIGAN; AND HEATHER LEATHAM

Ontario Tech University
Oshawa, ON, Canada

CONTENTS

Title: Digital Privacy: Leadership and Policy

Editors: Lorayne Robertson & Bill Muirhead

Front cover—design by Chris D. Craig, photos by P. Deligiannidis (tech) and J. Dent (privacy).

Format: eBook

First published in 2022 through the University of Ontario Institute of Technology. Note: Ontario Tech University is the brand name used to refer to the University of Ontario Institute of Technology.

Recommended APA 7 citation:

Robertson, L., & Muirhead, B. (Eds.). (2022). *Digital privacy: Leadership and policy.* Ontario Tech University.

This project is made possible with funding from the Government of Ontario and through eCampusOntario's support of the Virtual Learning Strategy. To learn more about the *Virtual Learning Strategy* visit: https://vls.ecampusontario.ca.

Open License

ACCESSIBILITY STATEMENT

Dr.'s Robertson and Muirhead, supported by eCampus Ontario and Ontario Tech University (UOIT), believe that education should be readily available to everyone, which means supporting the creation of accessible, open, and free educational resources. Wherever possible, the *Digital Privacy* open textbook adheres to levels A and AA of the Web Content Accessibility Guidelines (WCAG 2.0, 2.1) of perceivable, operable, understandable, robust, and conformance (https://www.w3.org/TR/WCAG21/). Pressbooks was chosen for its commitment to built-in accessibility, outlined at https://pressbooks.org/accessibility/. Further, we completed Coolridge et al.'s (2018) Checklist for accessibility during the final editing phase of book construction (available upon request).

1.

DIGITAL PRIVACY

Lorayne Robertson and Bill Muirhead

This chapter will assist students to:

1. Articulate why it is important to study digital privacy in education.
2. Understand the pedagogical foundations and commit to participating in the course.
3. See the overview of the e-book Digital Privacy: Leadership and Policy.

Why Study Digital Privacy in Education?

Throughout the chapters of this book on digital privacy in education, we will argue that digital privacy is a topic that is important to study and understand. First, we want to raise awareness of the breadth of surveillance in society today and to encourage students to question how much surveillance is normative and if they can accept that. In later chapters, we discuss the mechanisms for behavioural tracking and explain the mechanisms through which advertising is tailored to us as individuals and the magnitude of the corporate monopoly on curated advertising and content. We encourage students to take a critical stance and ask how comfortable they are with this level of exploitation of our summative individual preferences.

It is important to acknowledge that many students have not lived during a time when digital technologies were not pervasive. They may have almost no knowledge of what it feels like to be a private person. They may have no understanding that enables them to question how they are internalizing and acting out social norms established through the dictates of social comparison.

People seeking digital privacy want the ability to ensure that the collected information about them can only be used for the purposes to which they have agreed and at the time that the information was collected. This may

seem to be a lofty ideal, but it is an essential part of the vision for digital privacy in education. Canadian youth are beginning to explore their personhood, and they have the right to define who they are as adults without having to respond to the images and information about their youth or their formative moments.

Solove (2004) argues that the digital biographies that are being created about our personhood at present are unauthorized, partially true, reductive in nature and represent "impoverished judgements" of ourselves (p. 48). It is unfortunate that Canadians have to live with online biographies that do not allow them to unveil only those parts of themselves that they choose to show to others when they choose to do this. It is also unfortunate that the present system of digital privacy does not allow people access to the full digital dossiers that have been collected about them. Solove argues that privacy decisions are made for people who are frequently excluded from the process. Likewise, he argues that choices to relinquish data are no longer actual choices in today's economy (Sololve, 2004). We encourage students accessing this Digital Privacy: Leadership and Policy e-book to raise questions about these issues and the need for general policies for data protection in Canada.

Privacy as a Construct

Privacy is both a social construct and a historical construct. By this, we mean that our understanding of privacy is a collection of ideas that have taken shape over time. The context impacts the definition of privacy. At one time, privacy meant something quite different than it does today. Consider the scenario from an earlier era where a family takes pictures from an analog camera. The pictures are developed and saved in a box or an album. The parents had the security of knowing that these pictures of their children would only be shared with their consent. Their daughter did not have to worry that her three-year-old self would be seen in a later decade and shared with others unless she chose to share that physical copy of the photo. Privacy in this context has an expectation of privacy unless consent to share has been given.

Now fast track to the present where people have become digital persons (Solove, 2004). Details about people and choices in their lives are preserved permanently in giant databases that track their behaviour. In their wallets are credit cards, loyalty cards, health cards, bank cards and other cards that track and record where they are and what they are doing. Computers and devices routinely track every aspect of people's preferences and what they have searched online. Digital surveillance not only occurs online but increasingly cameras track our movements and this data is too digitized and linked to online profiles. If people are on social media, other people and not just computer databases are following their day-to-day actions and reactions. Now they are not only physical people but, according to Solove (2004), they have become digital persons complete with digital dossiers compiled by computer networks.

Nonetheless, we define digital privacy as an expectation of privacy unless informed consent has been given. This definition asserts that even digital persons can exercise some discretion with respect to how and where they share their digital information.

> **Digital privacy** is an expectation of privacy unless the user has given consent that includes an awareness of the risks associated with online services, and individual control over the collection, distribution and retention of personal information (Robertson & Muirhead, 2019).

How Technology Has Changed Everything

Life online has become much more routine since the declaration of the global pandemic in 2020. For the first time, students spend more time online outside of school than in school. The spread of the internet has become global but still concentrated. In the top 38 countries reporting any internet usage, more than 80% of those populations report being online (Internet users, 2016). This internet participation brings with it both affordances and risks, and some of the risks are to privacy and security. Another key construct to consider is that of personally identifiable information or PII. This is information that is used to identify a person distinctly—it is linked to a person's identity. Some elements of PII include name, country of origin, race, religion, age, gender identity, and sexual orientation. Other information can include education, health, criminal history and employment history. People are identified through symbols such as a phone number or postal code as well as biometric data such as fingerprints and blood type.

To put digital privacy in a very simplistic sense: technology facilitates the collection, distribution and storage of PII. Commerce seeks to maximize PII collection and use it to target advertising to specific groups. Consumers want to know that their privacy rights are protected despite the reality that they freely provide their PII. This creates a privacy paradox, which is one of the constructs that we study in this course.

Deliberate Pedagogical Design

This e-book is designed to accompany students and instructors undertaking the course: Digital Privacy: Leadership and Policy. There are four modules in this 12-week course and each module is intended to take the same amount of time: three weeks. Each module can stand on its own or be reviewed as a stand-alone resource.

The four modules of the Digital Privacy: Leadership and Policy course are:

1. Digital privacy in educational contexts.
2. Privacy in our daily lives: Legal and policy implications.
3. Digital privacy tools and technologies.
4. Wrapping up the course with a case study.

We have designed this course with a moderate degree of structure because some research (e.g., Eddy & Hogan, 2014) and our own experience tell us that courses with a mid-level of structure are more helpful to a wider range of students. Here are the mid-level structural elements that have been designed into the course:

1. Alignment of the learning objectives with the learning activities, readings and assignments,
2. Flipped classroom,
3. Distributed learning
4. Collaboration and Community
5. Critical pedagogy

In the next section, we explain each of these elements of deliberate pedagogical design.

A: Alignment of Learning Outcomes with the Activities and Readings

The learning outcomes for the Digital Privacy: Leadership and Policy course are listed in the course outline. Keen observers will notice that each of the learning outcomes has been addressed at least ten times throughout the course's four modules. In simple terms, here are some of the outcomes.

Upon completion of the course, students should be able to:

1. Articulate what they have learned and show connections between theory, evidence and practice.
2. Use a wide range of technology for communication.
3. Critically assess the affordances and constraints of technology and make evidence-based decisions about the best ways to use technology.
4. Critically evaluate information in the course and how digital technology impacts and is impacted by society and communities.

5. Prepare materials to educate different audiences.
6. Engage in ongoing reflection and debate and show the ability to make complex decisions.
7. Demonstrate integrity and ethical behaviour.

Our goal in designing the course was to have students return continuously to these learning outcomes multiple times. Accordingly, the outcomes are reflected in all of the course modules, readings and assignments.

B: Flipped Classroom

The Digital Privacy: Leadership and Policy course is designed to have elements that are studied by students before, during and after class. According to Eddy and Hogan (2014), moving much of the information transmission to before class has been found to free up 34.5% more time during class to reinforce major concepts, higher-order thinking and study skills. This strategy allows students to spend as much time as they need to fully prepare for class. Engaging students in preparing for the course in advance of the class promotes academic achievement and is significantly helpful for learners who are first-generation post-secondary students (Eddy & Hogan, 2014). Below is a quick overview of how this works.

Before class: Students review the slides for the class and study the assigned readings in order to prepare for class. In this way, when they come to the online, synchronous class, they have accessed the knowledge for that topic and are better prepared for discussions and other in-class activities. The readings for this course have been carefully selected to align with the course learning outcomes. Knowing that some students are keenly interested in this topic, we have provided additional readings at multiple points. Pre-class preparation may also include videos and activities.

During class: The Instructor assumes that the students have reviewed the slides and they are familiar with the readings. Accordingly, the instructor spends less time providing information so that more of the class time is dedicated to:

- Understanding students' experiences with this digital privacy topic,
- Applying the knowledge learned to real-life scenarios,
- Engaging in academic discourse and problem-solving on the topic.

After class: Students are assigned coursework to complete after class. This includes preparation for the next week and assignments.

C: Distributed Learning

Distributed learning (also called the pacing effect) is an element of moderate structure in a course that paces students' learning. It is the opposite of cramming at the last minute and hoping to pass the course. Better learning occurs when the learning opportunities are spaced apart rather than happening close together. When learning is spaced apart, it is more likely to have the students' attention and they are more likely to connect it to other contexts (Carpenter, 2020). Students spread out the time they spend on a concept with pre-reading activities, in-class assignments, and post-class reviews. This has a direct impact on how well they perform in the course (Eddy & Hogan, 2014). Distributing the learning also allows the students to cycle back to the key concepts in a course frequently.

This course has some cumulative assignments related to the case study. Students craft a plan for a case study and receive feedback. Throughout the course, they identify policies related to their case study and seek solutions. They present their case study to the other students and then use this case study as the basis for their final, collaborative paper. Giving early feedback helps to build a student's sense of safety that they are "on the right track." The second assignment builds on the first, and the final assignment is a culmination of their learning in the course. Rich asynchronous feedback with synchronous discussions between the instructor and student that mimic the established *office hours* of old combine to create an environment where instructor and students are engaged in a context of learning together and exploring in unison.

Synchronous discussions between the instructor and student that mimic the established *office hours* of old create an environment where instructor and students are engaged in a context of learning together and exploring in unison.

D: Collaboration and Community

More and more, instructors are moving away from teacher-centred pedagogies, where the instructor is the source of information. In this course, we rely on the students to research topics thoroughly before class and come to class with a good understanding of the topic and key questions. In this way, students can add their prior experience to the discussions. It is important to design learning activities in the course where students interact and share knowledge.

Social presence is a key element to deeper cognitive engagement, critical thinking, and student success.

Students in online courses are encouraged to share their cameras and their voices so that others can get to know them. Garrison (2009) describes social presence as "the ability of participants to identify with the community (e.g., course of study), communicate purposefully in a trusting environment, and develop interpersonal relationships by way of projecting their individual personalities" (p. 352). Garrison (2011) explains further that, "where social presence is established, students will be able to identify with the group, feel comfortable engaging in open discourse, and begin to give each other feedback" (p. 33). We would argue that social presence is a key element to deeper cognitive engagement, critical thinking and student success.

Another deliberate element of the design of this course is collaboration. Johnson et al. (1994) first defined collaborative learning through the concept of positive interdependence. This is where group members assume responsibility for ensuring that the group is successful and students, in turn, can depend on other group members to do their part. This course was designed to encourage students to develop both social presence and collaboration skills.

Earlier models of online learning had fewer opportunities for collaboration in real-time. Today's technologies allow students to participate in courses and share dialogue, video and images. They can use multiple communication channels simultaneously, such as using the Chat as a backchannel to ask questions or affirm comments in a way that does not interrupt the flow of the discussion in class. Google's G-Suite allows students to collaborate in real-time for document creation or asynchronously. Some students use quasi-synchronous forms of chat, such as WhatsApp, that allow real-time responses or responses with a short delay. According to Dalgarno (2014), these affordances allow students to engage more deeply with the topic.

E: Critical Pedagogy

Note. Child homeschooling, by C. Jorgensen, 2021.

In this text, the authors have taken a critical stance toward interrogating the concepts of digital privacy and surveillance in education. We have recognized that, as Apple (1999) has stated, much of our understanding has come from the dominant cultural groups in society. Kincheloe (2008), a critical pedagogy scholar, argues that we have assumed that what we have learned in school and the academy is inherently what is "best" for students. Critical scholars know, however, that our schooling history had gaps and omissions. There are other ways of knowing and other experiences that were left out of traditional education. This preferential treatment of colonial, patriarchal, monocultural knowledge was presented as "neutral" but it has negatively impacted the education of members of marginalized groups. Processes considered "best practices" may not be the most inclusive educational practices. In order for change to happen, teachers must become researchers and question past assumptions. Educator-researchers also need to interrogate past practices where teachers were considered the deliverers of information that may have represented a singular reality or an oversimplification of issues that require complex complicated considerations. One key to questioning dominant perspectives is to see how power is linked to the political economy and to examine its effects on individuals who are at different social locations (Kincheloe, 2008). Accordingly, in this e-book, the authors examine digital privacy in education in its complexity and encourage educator-researchers to interrogate assumptions within what Garrison (2011) has described as a community of inquiry.

Freire's (2007) pedagogical approach encourages students not to accept that "what is" is the way that it will always be (p. 84). His pedagogy encourages the cultivation of a critical consciousness in his students, where they seek to understand the social, political and economic contradictions. Freire encouraged individual empowerment for social change (Freire, 2007). We take a similar approach to student empowerment in the Digital Privacy: Leadership and Policy course and in this accompanying e-book. In Chapter 2, for example, Robertson and Corrigan question the dominant narratives surrounding youth surveillance in education and encourage instead an approach where students, parents and schools share responsibilities. In Chapter 4, Robertson and Muirhead present a critical policy analysis framework that encourages educator-researchers to examine whose perspectives have been considered and whose are missing in policy design and implementation.

Policy paradoxes in Chapter 6 are inherently complex and contested. In the final chapter, Case Studies, we encourage teacher-researchers to explore digital privacy cases in their complexity and feel empowered to call for change and renewal.

How This e-Book is Organized

Here is a brief summary of the topics and the organization of this e-book:

Chapter 1: Introduction

In the *Introduction*, we describe and define Digital Privacy as a construct. We explain the pedagogical foundations of the e-book and introduce four pedagogical themes that underpin all of the modules of the course.

Chapter 2: Digital Privacy in Education

In Chapter 2, we discuss why *Digital Privacy* is important for education settings and talk about the roles of teachers, learners, boards, colleges, and institutions of higher education in digital privacy. Some key terms are introduced, such as Duty of Care while we talk about the vulnerability of students online.

Chapter 3: Case Studies

In Chapter 3, the focus is on *Case Studies*, defining them and explaining how they work. Characteristics of great case studies are reviewed, and students can find more ideas about how to present a case study.

Chapter 4: Critical Policy Analysis

Chapter 4 introduces students to *Critical Policy Analysis*, which is a framework for reviewing policies and procedures. In this chapter, the authors explore policy definitions and look at the processes by which policies are enabled. We examine who enacts policies and how policies take on a life of trajectory of their own. The authors also present a Critical Policy Analysis framework that helps students examine the fairness of a policy.

Chapter 5: Legislation, Policies and Procedures

In Chapter 5, we examine key elements of *Policies and Privacy Legislation*. We examine some key definitions shared by policies and compare policies in different jurisdictions (Canada, the United States and Europe). We also look at some examples of policies.

Chapter 6: The Privacy Paradox: Present and Future

In Chapter 6, we attempt to unpack the *Privacy Paradox* by defining it. We look at the factors involved in enabling privacy paradoxes and how they reflect our priorities and our values. We also look at the corporate harvesting of data and dig deeper into corporate ownership of social media platforms and how they monetize access to data. In this chapter, students are encouraged to reflect on their own levels of privacy and look at some tools for minimizing their exposure to online risk. Next, we look at the principles of Privacy by Design. We delineate some privacy competencies and discuss how educators might protect themselves and their students when working online and in social media.

Chapter 7: Digital Privacy Tools and Technologies for Communication

Chapter 7 delineates Digital privacy tools and technologies for communication and helps students become familiar with how to manage their digital footprint, how to protect their privacy while web browsing and raising awareness of digital privacy risks in the home.

Chapter 8: Today's Devices and Tomorrow's Technologies

In Chapter 8, *Today's Devices and Tomorrow's Technologies*, the author discusses the digital privacy implications for the use of smart devices, wearable technologies, the Internet of things (IoT) and other emerging technologies for the risks and threats to digital privacy.

Chapter 9: Educational Leadership for Digital Privacy

Chapter 9: *Educational Leadership for Digital Privacy* encourages students to *put it all together* and reflect on the different ways that they can show leadership in digital privacy. Students will be encouraged to consider

the key takeaways from the course and how they will affect their future practices in education, personal life and professional practice. In consideration of the future, students will be asked to consider how to share the responsibility to protect students' digital privacy.

Chapter 10: Under Construction: Case Studies and Scenarios

Chapter 10 – *Case Studies and Scenarios* are "under construction", as it will be authored by students who design case studies for this e-book. Every year, selected case studies that are sent to the authors can be added to this e-book.

References

Apple, M. W. (1999). *Power, meaning, and identity*. Peter Lang.

Carpenter, S. K. (2020). *Distributed practice or spacing effect*. Oxford Research Encyclopedia of Education. https://doi.org/10.1093/acrefore/9780190264093.013.859

Dalgarno, B. (2014). Polysynchronous learning: A model for student interaction and engagement. In B. Hegarty, J. McDonald, & S.-K. Loke (Eds.), *Rhetoric and reality: Critical perspectives on educational technology. Proceedings ascilite Dunedin 2014*, 673–677. https://ascilite.org/conferences/dunedin2014/files/concisepapers/255-Dalgarno.pdf

Eddy, S. L., & Hogan, K. A. (2014). Getting under the hood: How and for whom does increasing course structure work?. *CBE—Life Sciences Education, 13*(3), 453–468. https://doi.org/10.1187/cbe.14-03-0050

Freire, P. (2005). *Pedagogy of the oppressed (30th-anniversary edition)*. Continuum International. https://envs.ucsc.edu/internships/internship-readings/freire-pedagogy-of-the-oppressed.pdf

Garrison, D. R. (2009). Communities of inquiry in online learning: Social, teaching and cognitive presence. In P. L., Rogers, G. A., Berg, J. V. Boettcher, C. Howard, L. Justice, K. D. Schenk (Eds.), *Encyclopedia of distance and online learning* (2nd ed.) (pp. 352-355). IGI Global.

Garrison, D. R. (2011). E–Learning in the 21st century: A framework for research and practice (2nd Ed.). Routledge.

Internet users by country (2016). (2016, July 01). Internet Live Stats. (n.d.). https://www.internetlivestats.com/internet-users-by-country/

Johnson, D. W., Johnson, R. T., & Holubec, E. J. (1994). *The New Circles of Learning: Cooperation in the classroom and school*. Association for Supervision and Curriculum Development.

Jorgensen, C. (2021, January 13). *Child home schooling* [Photograph]. Unsplash. https://unsplash.com/photos/leyUrzdwurc

Kincheloe, J. L. (2008). *Critical pedagogy primer*. Peter Lang.

Robertson, L., & Muirhead, B. (2019, April). Unpacking the privacy paradox for education. In A. Visvizi, & M. D. Lytras (Eds.), *The international research & innovation forum: Technology, innovation, education, and their social impact* (pp. 27-36). Springer, Cham. https://doi.org/10.1007/978-3-030-30809-4_3

Solove, D. J. (2004). *Digital Person: Technology and privacy in the information age*. New York University Press. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications

2.

DIGITAL PRIVACY IN EDUCATION

Lorayne Robertson and Laurie Corrigan

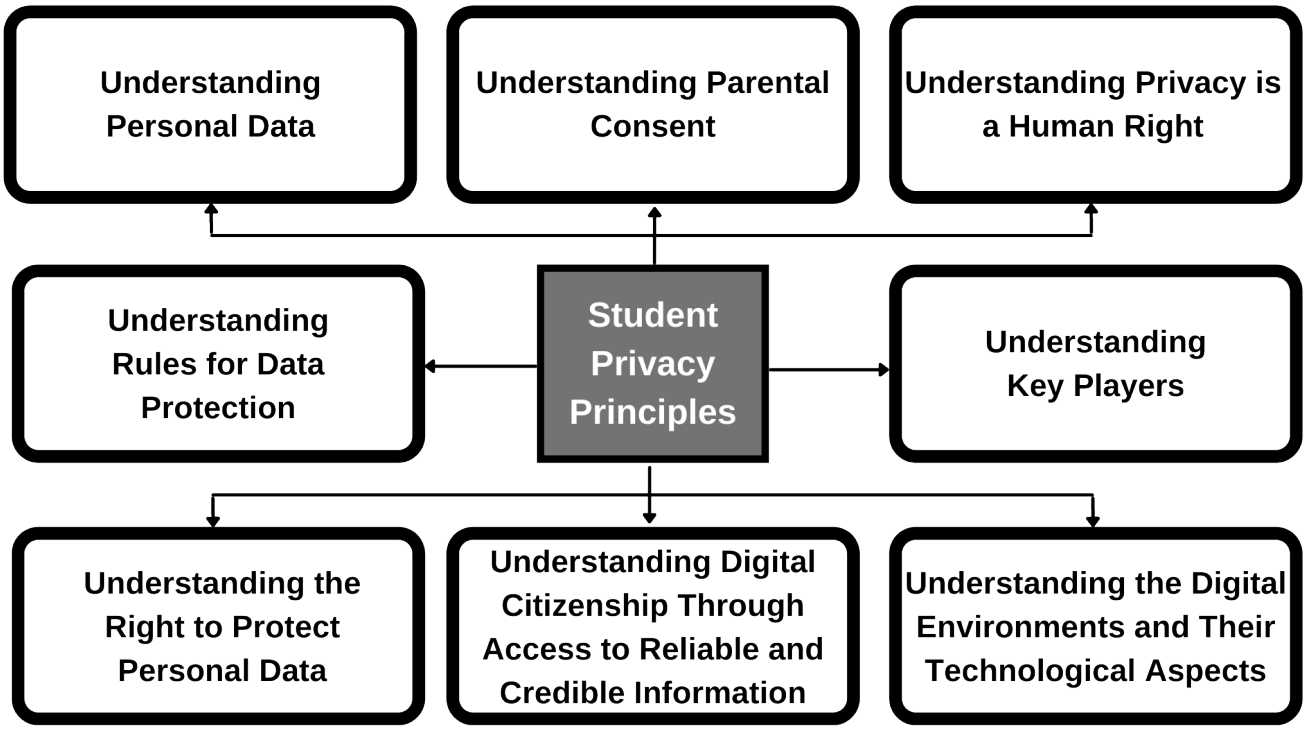
This chapter will assist students to:

1. Explain how changes in the digital landscape have impacted digital privacy in schools.
2. Critically weigh different approaches to building students' digital privacy capacity.

In this chapter on digital privacy in education, we explore how digital technology and artificial intelligence have greatly expanded both the opportunities for internet use and for increased digital surveillance. We examine the educational implications of data surveillance and consider the role of schools in an era that is characterized by the steady creep of passive data collection. Secondly, we ask questions of educators regarding the types of curriculum and policy responses that are needed. Finally, we argue for a much more critical examination of the role of digital privacy and surveillance in schools. Figure 1 outlines our reflection of student privacy principles in this chapter.

Figure 1.

Student privacy principles.



Digital privacy solutions for students are multi-faceted. Students need to understand what constitutes personal data and understand that privacy is a human right. They need to understand the context of the present digital environment, and that there are multiple players in the system who are looking to have access to their data or looking to protect their data. Students also need to acquire skills of digital citizenship so that they understand that information can be curated and mediated. They need to know how to access credible, reliable information. Finally, students need to understand why it is important to protect their personal information and why there are rules for data protection. Students of vulnerable ages need to know how to work with their parents' supervision in order to protect their data. In sum, the overall picture for digital privacy in education is complicated!

Key topics in this chapter are as follows:

1. The context (landscape) for internet use in Canada.
2. Connecting digital surveillance and digital privacy.
3. Protecting students' digital privacy as a shared responsibility.
4. Framing discussions about digital privacy in education.

1. Internet Use: The Canadian Context

Note. Person In a gray sweater on a laptop with facemask, by E. Akyurt, 2020.

In 2020, Canada was in the throes of a global pandemic, and Canadians were required to work from home and attend school remotely. Many changes in Canadians' internet usage occurred in the five years that led up to the pandemic and there were more changes during the pandemic. Statistics Canada (2021) reports that many Canadians considered the internet to be a *lifeline* during the first waves of the pandemic. Four out of five Canadians shopped online, and their online spending rose significantly (Statistics Canada, 2021). Four out of five Canadians watched streamed content, with 38% reporting that they watched more than ten hours in a typical week (Statistics Canada, 2021). Not surprisingly, more than two-thirds of Canadians used the internet to monitor their health (Statistics Canada, 2021). The statistics were clear also for young Canadians; the vast majority (98%) of young Canadians reported that they were using the internet (Statistics Canada, 2021). Smartphone use also increased with 84% of Canadians reporting that they used a smartphone to communicate (Statistics Canada, 2021). Almost half of this group reported that they check their phone every half hour (Statistics Canada, 2021).

The prevalence of devices such as laptops, Chromebooks, and cell phones with their related applications, as well as the emergence of smart home devices have done more than simply change the technology landscape. As technology has increasingly become such a big part of people's lives, the result has been a gradual decrease or erosion of Canadians' privacy. This is happening for multiple reasons. First, the users lack the time to read, understand and give informed consent, which we would define as consent with full awareness of the risks involved. The Office of the Privacy Commission defines meaningful consent as a knowledge of what information is being collected, the purpose for the collection, how the information will be shared, and understanding of the risks and consequences. Secondly, privacy agreements are long and convoluted. Third, with so many Canadians accessing the internet on their phones, and so many young people using the phone for social media, gaming and instant messaging, the fine print of privacy policies read on phones is so small that it almost necessitates click-through rather than a detailed study of the implications of agreeing to a disclosure of privacy. Even the Canadian Internet Registration Authority requires the download of an app and a series of instructions in order to provide users with screening tools for pop-up advertising on devices.

A critical examination of digital privacy requires stepping back and taking a deeper look at what is happening. Parents and educators also need to analyze what is happening, as they are the role models and imprinters for

their children and students who navigate the digital world. We argue in this chapter that Canadians must consider multiple threats to individual privacy. Some of these threats include the collection and marketing of personal data. Other threats involve increasing surveillance of youth by *trusted* adults without consideration of the implications of over-surveillance for their individual privacy.

Note. Person in front of red lights, by G. Bourdages, 2017.

In Canada, *The Office of the Privacy Commissioner* (OPC) was making recommendations to protect the online privacy of Canadian children as early as 2008 (OPC, 2008). The Privacy Commissioner urged providers of content for youth to ensure that young people visiting websites could read and understand the terms of use. The Privacy Commissioner website focuses on two aspects of online activity in youth: personal information protection and online identity and reputation. No legislation, however, has been presented in Canada to protect the information of children and youth, leaving children's privacy largely unprotected as it relates to educational content and policy. Central concepts of digital privacy such as *digital footprint, digital dossier* and *digital permanence* have not found their way into everyday curriculum policies.

Confounding the issue of digital privacy protection for children and adolescents is the patchwork of policy solutions. For example, Canada has devolved responsibility for education to the provinces and territories, which design operational and curriculum policies (Robertson & Corrigan, 2018). In Ontario, however, municipalities and cities oversee the protection of personal information. *The Municipal Freedom of Information* and *Right to Privacy Act* (MFIPPA; 2021) defines personal information as recorded information that can be used to find someone's identity. This recorded information about an individual includes the following areas and more: a) race, origin, religion, age, gender, sexual orientation, or marital status; b) educational, medical, psychiatric, criminal, or employment history; c) any identifying number or symbol; and d) address, telephone, fingerprints, blood type, and name. There is little in the MFIPPA policy to indicate that it has been updated to the digital realm, although it does acknowledge that a record could be electronic (1990, p. 3). MFIPPA states that institutions shall not use personal information in their custody (S. 31) unless they have consent (Robertson & Corrigan, 2018).

In summary, the context of digital privacy in Canada is one where reliance on the Internet for education, work and leisure is increasing. Digital/mobile applications require consent to use them, but the consent forms are lengthy and difficult to decipher. A patchwork of national, provincial and municipal services oversees privacy. The office of the Privacy Commissioner of Ontario provides advice, but there is little coordination evident

between the offices overseeing privacy and the provincial designers of curriculum and operations in education. There appears to be an agreement in policy that personal information should be protected, but there has been no pathway forward to design comprehensive privacy protection.

2. Pervasive Surveillance and Digital Privacy

Another key aspect of the present context is that of surveillance, which has become so much a part of our lives that it has quite literally become a backdrop to the everyday. In this section of the chapter, we discuss the collection of human experiences as behavioural data as one form of surveillance. In addition, we review how surveillance can also be packaged and sold as student safety measures.

Note. A painting on a wall warning visitors about video surveillance, by T. Tullius, 2020.

Recently, a colleague purchased potato chips with cash at a convenience store. The next day, when he received pop-up advertisements for chips on his home computer, he wondered if it could be a coincidence. Since he did not use a bank card or a credit card for the initial purchase, he thought his purchase was anonymous. He was unaware of the hidden workings of surveillance cameras in stores and how his phone and other devices were tracking his whereabouts. He was also unaware that data about his purchasing habits and location were potentially being captured and shared without his express consent. He was certainly not aware that data related to his purchasing habits were being sold and shared.

The New York Times Privacy Project made the claim that location data from sources hidden in mobile phone apps have made *an open book* of the movements of millions of Americans, as it is recording who and where they visit and for how long. Some of the data is recorded by unregulated and unscrutinized companies (Thompson & Warzel, 2019). Similar claims have been made in Canada that Google and Facebook are tracking users' search data for marketing purposes (Dangerfield, 2018). Key critical questions need to be asked and answered regarding the rights of individuals to privacy and the growing apathy and immobility to challenge digital surveillance for corporate gain.

The Center for Democracy and Technology in the United States has recently raised issues of pervasive student surveillance on school-owned computers distributed during emergency remote learning. In a letter to the US Senate, they suggest that,

> Student activity monitoring software can permit school staff to remotely view students' computer screens, open applications, block sites, scan student communications, and view browsing histories.

> It may utilize untested algorithmic technology to flag student content for review, and security flaws have also permitted school personnel to access students' cameras and microphones without students' permission or awareness. (Venzke & Laird, 2021, p. 1)

Haskins (2019) argues that almost five million students in the US are being watched online in schools by the surveillance industry and students do not have the opportunity to opt-out of being watched. She reports that Gaggle uses a combination of artificial intelligence and human moderators to track students' emails and their online work, including messages that come into the cloud-based learning site from social media. One of the concerns she raises is that LGBTQ words are on the banned words list. She also raises the overall concern that students are subject to *relentless inspection*. She questions if the cost of this surveillance reflects the real priorities of school districts (Haskins, 2019).

Hankerson et al. (2021) report that surveillance of student devices treats different groups of students differently. Students using the school's digital devices are monitored more than students with personal devices. Students from poverty are less likely to own personal devices and are therefore monitored more. Local education authorities in the United States are seeking student activity monitoring vendors to surveil students in the name of protection of digital privacy. Similarly, *Feathers* (2019) reports that, in the United States, schools use snooping tools to ensure student safety, but some studies looking into the impact of these tools are showing that they may have the opposite effect—such as damaging trust relationships and discouraging communities of students (e.g., LGBTQ) who look for help online.

Despite these reports, a survey for the Center for Democracy and Technology (2021) in the United States finds that parents and teachers acknowledge the privacy concerns, but they see that the benefits of student activity monitoring outweigh the risks (Grant-Chapman et al., 2021).

Fisk (2016) has raised different but equally important concerns about the surveillance of youth. As they have increasingly documented their lives online (e.g., through Instagram, TikTok, etc.), adult surveillance of their lives has increased to monitor many of the previously unsupervised spaces in their lives. Fisk has identified *pedagogies of surveillance* (p. 71) that observe, document and police the behaviours of youth. Parents, for example, use the tracking devices on their children's phones or fitness apps to monitor their whereabouts. Internet safety presentations are designed to destabilize parents' awareness of what youth are doing online and *sell* internet safety to parents and guardians. A critical examination of these practices asks: Who profits from these youth surveillance initiatives? Who are the winners and the losers? Do young people have a right to know when they are being monitored online?

Parents, for example, use the tracking devices on their children's phones or fitness

apps to monitor their whereabouts. Internet safety presentations are designed to destabilize parents' awareness of what youth are doing online and *sell* internet safety to parents and guardians.

Palfrey et al. (2010) at the Harvard Law school argue compellingly that youth need to have an opportunity to learn about digital privacy and acquire digital privacy protection skills. They explain in the following way,

> We also need to begin the conversation with a realization that adult-driven initiatives – while an important piece of the puzzle – can only do so much. Youth must learn how to handle different situations online and develop healthy Internet practices. Through experience, many youths are able to work out how to navigate networked media in a productive manner. They struggle, like all of us, to understand what privacy and identity mean in a networked world. They learn that not everyone they meet online has their best intentions in mind, including and especially their peers. As with traditional public spaces, youth gain a lot from adult (as well as peer-based) guidance. (Palfrey et al., 2010, p.2)

There are mixed messages with respect to who has the responsibility to teach and reinforce internet safety guidelines to protect students' privacy. MediaSmarts, which is a Canadian nonprofit, reports in one study (Steeves, 2014) that more students said that they learned about internet safety from their parents than from the school. Students say that their teachers are more likely to help them in other ways, such as helping them search for information online and how to deal with cyberbullying than to teach them about digital privacy. The reality is that parents cannot assume that teachers are addressing digital privacy and teachers cannot assume that parents are doing this. Digital privacy education is a shared responsibility.

Note. Green binary code, by M. Spiske, 2018.

Students may not know that their *digital footprint*, which is the list of all the places they have visited online, is searchable and can be connected back to them. Some of the data is collected actively, through logins. Some of the digital footprint, such as which websites are visited and for how long, is collected passively as they are web surfing—this data is called *clickstream data* because it shows where a user has navigated online (Solove, 2004). Another means of passive data collection is through cookies or tags which are small sets of codes that are deployed into the user's computer when they visit a website.

One company capitalizes on clickstream data via DoubleClick, which accesses cookies on the user's computer,

looks up the person's profile and then sends advertisements targeted specifically for that person in milliseconds. Hill (2012) explains how one company, Target, looked over customers' purchases and predicted whether or not they might be pregnant. After a father complained that his daughter was receiving targeted baby product ads, the company began disguising this targeted advertising by putting ads for lawn equipment beside the baby ads. In 2004, DoubleClick had more than 80 million customer profiles (Solove, 2004). This changed significantly when Google purchased DoubleClick.

According to Lohr (2020), the acquisition of DoubleClick by Google in 2007 was a significant game-changer for Google because Google in 2007 was one-tenth of the size that it became by 2020. At present, Google owns the leading browser globally with accompanying email, meeting space and other software, but the source of most of its tremendous profits is its advertising (Lohr, 2020). The dominance of Google has led to investigations by the Justice Department (Geary, 2012; Lohr, 2020) and the filing of an antitrust lawsuit on its search engine in October 2021. Hatmaker (2021) reports an additional antitrust lawsuit over Google Play was filed in July 2021.

According to Geary (2012), DoubleClick (Google) operates two categories of behavioural targeting. For the first, a website owner can set a DoubleClick cookie to track which sections of their website you are browsing. DoubleClick also tells advertisers how long the ad is shown and how often it will appear to the user. Secondly, Google runs Adsense, where different publishers pool the information from browsers; this is third-party advertising. The two systems can work together to categorize the person's ad preferences. Categories are established to help advertisers target directly to you. As a user, you can visit Google's ad preferences manager to see how your preferences have been categorized.

Students also may not understand *digital permanence*, which is the understanding that data posted online is very difficult (impossible) to delete. Students may not be aware that inappropriate or thoughtless messages posted today can impact future employment. They may also not be thinking that humour to a pre-teen may not be the humour they will appreciate when they are older. Some studies show that young people do care about privacy and want to protect their information (Palfrey et al., 2010; Steeves, 2014). The issue remains, however, that there is no clear national direction or consensus on the protection of personal information that also limits the degree of passive surveillance permitted by law.

The collection of information about us without our consent is not a new phenomenon. According to Solove (2004), in the 1970s, the American government started selling census data tapes. They sold the information in clusters of 1500 homes with only the addresses (no names). Marketing companies matched the addresses using phone books and voter registration lists (Solove, 2004). Within 5 years, they had built databases for over half of American households (Solove, 2004). In the 1980s, they wanted to add psychological kinds of information about beliefs and values, which led to the creation of taxonomies of people groups who had income, race, hobbies and values in common. By 2001, the marketing of these databases, which allows advertisers to target

your mail, email or phone through telemarketing, grossed over $2 trillion in sales (Solove, 2004). Yet, it is not possible to sign up for a bank account or a credit card without offering up much of your personal information (Solove, 2004).

> ***Surveillance capitalism*** is a practice that claims that human experience is free material for hidden commercial data extraction, prediction, and sales.

Zuboff (2020) argues that a new economic logic is now in place, which has been relatively unchallenged through policy. She defines *surveillance capitalism* as a practice that claims that human experience is free material for hidden commercial data extraction, prediction, and sales. These practices are allowed to proliferate because the dangerous illusion persists that *privacy is private* (Zuboff, 2020). In surveillance capitalism, human experience is captured by different mechanisms, and the data are reconstituted as behaviour. This data capture is allowed to continue when customers give up pieces of themselves and when pieces of their information are taken from them without their knowledge. This concentrates wealth, knowledge and information in the hands of a few for profit. For example, Facebook produces 6 million predictions every second for commercial purposes. No one could easily replicate Facebook's power to compile data (Zuboff, 2019).

According to Van Zoonen (2016), the general public is complicit in releasing their information. Despite indicating that they have privacy concerns, they use simple passcodes and share these codes among devices. They share their personal information on social media sites and, in general, while they do not believe that their nationality, gender or age is sensitive information, they are increasingly concerned about how data might be combined for personal profiles. They want to weigh the purpose of the data collection and assess whether the benefits outweigh the risks. The request for too much data, for example, might outweigh the benefits (Van Zoonen, 2016).

The protection of personally identifiable information for youth is even more important because they are learning the skills toward understanding consent. Also, schools may be unknowingly complicit in providing third-party access to student information through educational apps. It makes sense, therefore, that schools should guide students in the reasons behind protecting their digital privacy and help them to understand it (Robertson & Muirhead, 2020).

Some key lessons about digital privacy for Canadian students in the 21st century to understand include:

- how their data is being collected and for what purpose,
- how long their data will be retained,
- what constitutes informed consent, and
- the difference between voluntary and passive data capture.

3. Digital Privacy as a Shared Responsibility

Digital technologies are advancing at such an unprecedented speed that neither the curriculum nor the general policy guidelines in education can keep pace, resulting in curriculum and policy gaps surrounding digital privacy in education. The protection of personally identifiable information (PII) has a different level of importance for youth because there are greater risks for their safety and their age may make them less able to give informed consent. Without a clear understanding, schools and school districts might be unknowingly complicit in providing third-party access to student information through educational apps. It makes sense to put in place an expectation that students who use technology in schools also need opportunities to gain an understanding of digital privacy. In the United States, for example, the Children's Internet Protection Act requires schools that receive funding for technology must also provide students with education about online behaviour (Federal Communications Commission, 2020).

Note. Connected world, by NASA, 2015.

A Global Privacy Enforcement Network (GPEN) was established in 2010 (GPEN, 2017) composed of 60 global privacy regulators. These experts cautioned that teaching platforms that are internet-based can put students at risk for the disclosure of their personal information. In a 2017 review, GPEN found that most online educational apps required teachers and students to provide their emails to access a particular educational service or app, thereby providing a link to their PII. *Only one-third of the educational apps reviewed allowed the teachers to create virtual classes where students' identities could be masked* (GPEN, 2017). Although teachers complied with requests to provide the students' actual names, they found that it was difficult to delete these class lists at the

end of term. While most of the online educational services restrict access to student data, almost one-third of the educational apps reviewed in the GPEN sweep did not provide helpful ways for students to opt-out or to block third party access to their data (GPEN, 2017) taking away their right to make a privacy decision, let alone an informed privacy decision.

The findings of the GPEN sweep are understandable given the speed at which educational apps have proliferated. The curriculum has not been able to keep pace. There are a number of key understandings that **have not been a part of the school curriculum** for generations of digital users. According to a Canadian policy brief (Bradshaw et al., 2013), here are some examples:

1. ***Personally-identifiable information*** *(PII)* – Students should also understand what constitutes PII as this can vary from person to person. Bradshaw et al. (2013) identified four common categories of privacy-sensitive information:

    - Personally-identifiable information: such as the name of the user, credit card numbers and IP addresses.
    - Lifestyle information: such as race, religion, relationship status, sexual orientation, political affiliations, friends and family members.
    - Behavioural data: such as viewing habits, websites visited and time spent; online purchases, store loyalty programs and credit cards.
    - Unique device identifiers: such as user location, determined by globally unique identifiers connected to mobile devices.

2. ***Passive data capture:*** Students, teachers and parents need to understand different forms of data capture. Passive capture happens when data is taken without the knowledge of the person. Other data is shared with permission.

    In the present era, it is sometimes hard to distinguish between these two. For example, if a person wishes to use the store's wifi, they might *click-through* the privacy agreement without reading it. By doing this, they are agreeing to broader data capture, such as where they pause in the store to look at merchandise. Some third-party applications that collect student data may require parents to *click through* the privacy agreements. These agreements tend to be long and difficult to understand. This prevents parents from gaining a clear and concise explanation of the implications of sharing their children's data.

    Note. Free WiFi inside, by B. Herman, 2018.

3. ***Data recombination***: While people are generally careful about sharing their credit card information and personal identifiers, they may not be aware that they are also passively sharing other information

that can reveal their identity. For example, small amounts of simple demographic information can be recombined in order to identify a person uniquely. In one study, postal code, date of birth and gender were combined to identify 87% of Americans uniquely (Sweeney, 2004). Movie preferences can generate similar identifications (Ohm, 2010). This is a consequence of data recombination that occurs when large amounts of data are collected and sold in a largely unregulated online marketplace.

4. ***Behavioural micro-targeting***: This is a technique that targets future advertising to potential customers based on an analysis of website use. Companies track digital transactions and websites visited, aggregate the data and sell the information for political or advertising purposes. Google (owner of DoubleClick discussed earlier in this chapter) announced that this was being undertaken to make advertising more relevant for its users (Wojcicki, 2009). Geary (2012) writes that Google claims that tracking people gives them the benefits of making the advertising more relevant, controlling how many times the user has to see the ad and also allows a way for *savvy web users* to control and block advertisers (Geary, 2012).

5. ***Loyalty apps*:** Students need to be made aware that loyalty cards collect more than the points that they advertise in order to draw in customers. McLeod (2020) reported that his coffee order app had located his whereabouts both at his home and work address. This occurred when he was in Canada and on vacation. Through combinations of networks, the app tracked him throughout the day and night—in total reporting his location 2,700 times in five months. He had incorrectly assumed that the app was working only when he was ordering his morning coffee (MCleod, 2020).

Note. Scrolling apps, by R. Hampson, 2017.

These examples illustrate that understanding consent is a central concept in understanding digital privacy.

PIPEDA: Canada's regulatory guidelines for obtaining meaningful consent are outlined in the *Personal Information Protection and Electronic Documents Act* (PIPEDA; 2016). This legislation regulates privacy for the private (commercial) sector in Canada and is not specific to education or youth. In comparison, the American *Children's Online Privacy Protection Rule* (COPPA; 1998) designates the age of 13 as the minimum age for young persons to have an online profile. This legislation was designed to protect young internet users, but recent research shows that there are many underage users on the internet, raising questions about whether or not legislation is the answer (Hargittai et al, 2011).

There is a gap in the national legislative direction in Canada that is designed to protect the personal information of all Canadians, including young people. There are also key understandings that should become part of basic education on internet use.

While **PIPEDA** does not provide privacy guidance, it regulates the commercial sector through key principles for *fair information practices*. These are as follows:

Notice: Users should be informed when information is collected, for what purpose, how long it will be used, and how it will be shared.

Choice: Users should have a choice about whether or not they share their information.

Access: Users should be able to check and confirm their information on request.

Security: The users' information should be protected from unauthorized access.

Scope: Only the required information can be collected.

Purpose: The purpose for collecting the information should be disclosed.

Limitations: There should be a time limit on how long the information will be held.

Accountability: Organizations should ensure that their privacy policies are followed.

In California, a *Shine the Light* (2003) law requires list brokerages to tell people on request where they have sold their personal information (Electronic Privacy Information Center, 2017). To the best of our knowledge, no similar legislation exists to protect the digital privacy of Canadian children and adolescents. Chen examined the digital divide in Ontario schools and notes, "to date there is no national policy on digital learning in place" (Chen, 2015, p.4). Without a systematic approach to digital learning, the school districts are left to define digital curriculum learning outcomes on their own. While education falls to the provinces and territories, the Annual Report of the Information and Privacy Commissioner of Ontario (IPC) (2020) does not give direction to education in Ontario. The Ontario Government report: Building a Digital Ontario (2021) does not address digital privacy in education. Recently, the Ontario government has made clear that digital privacy policies and terms of use are the responsibility of local school districts (Information and Privacy Commission for Ontario, 2019; Ministry of Education, 2020).

One province in Canada, Ontario, has written a policy (Bill 13) that holds students accountable for their online activities if they impact other students negatively. *Bill 13*: *The Accepting Schools Act* (2012) requires schools to address harassment, bullying, and discrimination using a number of interventions that include suspension and expulsion. Specifically, it identifies cyberbullying behaviours, such as the online impersonation of others, and makes digital bullies subject to the consequences enacted in the legislation, including suspensions, expulsions, and police intervention. While the scope and sanctions of the Accepting Schools Act have given schools the authority to respond to cyberbullying and online aggression, it does not focus on or include language that develops the digital citizenship of students. It also does not address the professional development of teachers who, ten years after its assent, now teach students who are even more immersed in the technologies that can lead to school-based consequences.

Shared Responsibility

The *Organization for Economic Co-operation and Development* (OECD) has 38 member countries, including Canada. They have published a Typology of Risks (OECD, 2021) for children in the digital environment. There are content, conduct and contact risks as well as consumer risks. They identify cross-cutting risks as those that include all four of the risk categories. The three cross-cutting areas are *Privacy Risks, Advanced Technology Risks, and Risks on Health* and *Wellbeing* (OECD, 2021).

Recognizing that the teaching of digital privacy is a shared responsibility, the *Office of the Privacy Commissioner of Canada* (OPC) (2022) has produced materials to encourage this shared responsibility. There is a graphic novel, Social Smarts: Nothing personal!, a downloadable resource in which a phone guides a student through the online world. It is aimed at youth 8-10 years old. In addition, the OPC co-sponsored a global resolution on children's digital rights [PDF]. There is a highly informative blog post for parents entitled *Having a Data Privacy Week 'family tech talk'* with suggestions on how to protect child privacy and recommendations for how to have tech talks.

There have been other, international responses regarding the shared responsibility to keep children safe online. In the UK they have created a *data protection code of practice* (OPC, 2022), called the Age Appropriate Design Code, which requires internet companies to respect children's rights, act in their best interest, and make products safer for children.

4. Framing digital privacy discussions for schools

There are some key considerations that can frame discussions about digital privacy in schools.

Duty of Care: Teachers and administrators have a duty of care under the Ontario Education Act that requires them to be positive role models for students and act as a kind, firm and judicious parent would act to protect them from harm. This standard of care varies depending on the type of activity and the age of the students. The younger and less experienced students would require closer supervision (Berryman, 1998). The protection of *personally identifiable information* (PII) for youth has a different level of importance because there are greater risks for their safety and their age may make them less able to give informed consent.

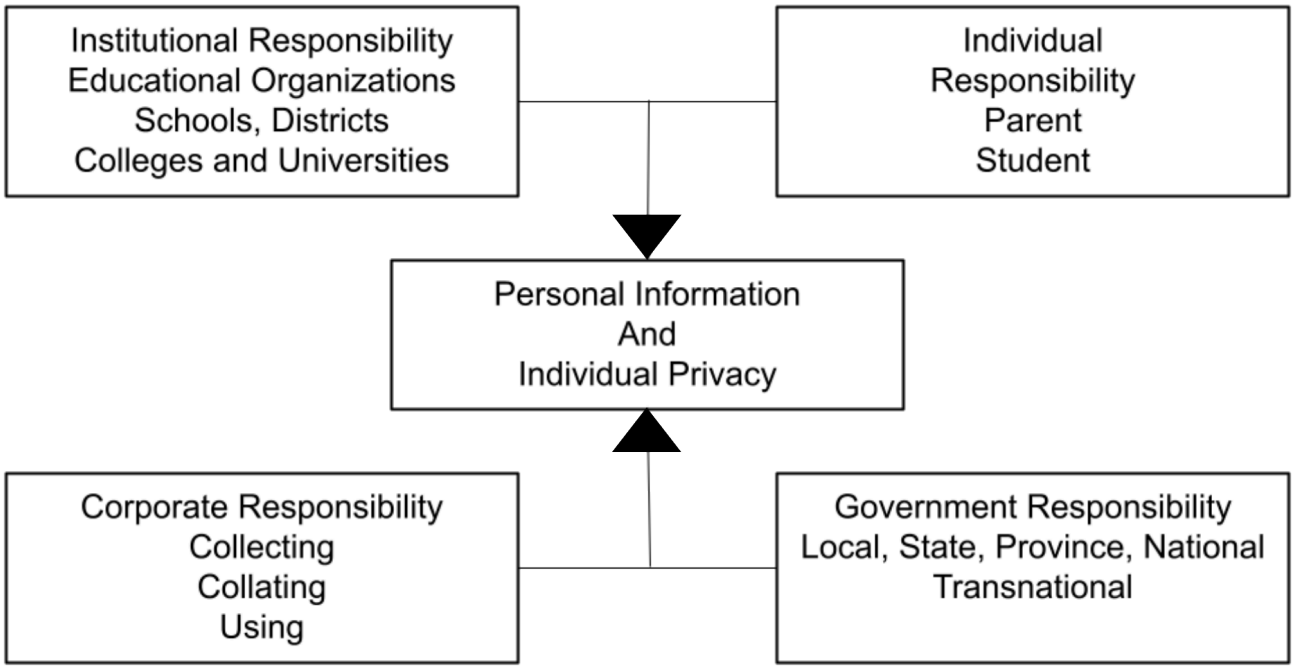
Policy Patchwork: First, educators need to be aware that they are operating in a policy forum that has multiple policy designers at different levels such as the school, educational authority or district level, provincial level and national level. For example, the Office of the Privacy Commissioner of Canada has lessons for students in Grades 9-12 that are based on privacy principles from the *Personal Information Protection Acts* that guide Alberta and British Columbia, *An Act Respecting the Protection of Personal Information in the Private*

Sector from Quebec, as well as PIPEDA (a national Act, described earlier in this chapter). The lesson is designed to teach students about their rights to privacy. It provides a self-assessment for students to understand how well they understand privacy and shows them how to make a privacy complaint.

Rights to privacy: Secondly, students need to be informed about the degree of surveillance operating somewhat unregulated at present and how this has implications for their safety as well as their right to information (e.g., news and websites) that has not been curated for them. If the provincial curriculum policies do not require students to learn about the protection of PII, the implications of their digital footprint and digital permanence, then school districts or authorities will need to find ways to address this gap. The curriculum should be based on the provision of information about the right to privacy, how students can take action to protect their personal information and their rights to recourse when they are being monitored or the information (news) they seek is being curated. For example, the PVNCCDSB, an Ontario school district, has developed a Digital Privacy Scope and Sequence from Kindergarten to Grade 12 that supports student privacy alongside the acquisition of digital skills. From the importance of using correct passwords to curating a digital footprint, students learn the skills with the instruction of

Shared responsibility: In this chapter, we have advocated that the protection of personal information and individual privacy is a shared responsibility. First of all, the educational institutions, such as the school districts or school authorities, the colleges and universities share an institutional responsibility to create policies that are clear and understood by their students. Corporations that use data for marketing purposes need to be more transparent about how they collect data and provide easy opt-out solutions. Governments have the responsibility to create digital privacy policies that protect citizens from corporate profit and overreach. Finally, individuals, parents, students and educators have the responsibility to educate themselves on the topic of digital privacy.

Figure 2.



The International Competency Framework for Privacy Education

A consortium of international data protection commissioners wrote a framework for teaching about data protection, the International Competency Framework on Privacy Education. Their intent was not to put the responsibility for teaching about data protection on the schools, but they wanted to share their expertise by developing a framework of digital competencies (International Working Group on Digital Education, (IWG), 2016).

The commissioners did not match the framework to specific legislation but designed the competencies so that they would function irrespective of jurisdiction. Their goal was to create an international base of common knowledge and skills on digital privacy for education and distribute this information for the benefit of students and schools. This framework focuses on empowering the digital student and encourages them to work with a responsible adult. It takes into consideration research that youth do care about their privacy (e.g., Palfrey et al., 2010) and that they need to work together with concerned adults such as their parents and teachers to build their skills in a digital era. (Robertson & Muirhead, 2020).

Here is a summary of the nine guiding principles in this International data competency framework:

1. Students should understand the concept of personal data. They should know that personal data is any

data that identifies an individual. Students should learn how to discern which information is particularly sensitive, something which can vary from country to country. They also need to know how their online presence can be traced back using technical data and metadata.

2. Students should understand that *privacy is a human right* that should be protected. They need to know how their actions can affect their own privacy and the privacy of others.
3. Students need to understand the digital environment's *technical aspects* and how digital space is structured. This includes an understanding of the risks associated with the digital space and what is meant by digital security. Students should also learn how to ensure the security of their own digital environment.
4. Students should understand the digital economy of service providers and terms of use. They need to know the *key players* in the digital environment, and how personal user preference files are established. Student users need to know what data is collected and stored while online.
5. The fifth principle is the understanding that there are some key rules which are important for *data protection*, such as people's rights to be informed about who is collecting their personal information, for what purpose, and how long data will be stored. End users also need to know how to work with data protection authorities.
6. Students should understand key aspects of personal data regulations and the necessity to manage the use of *personal information*. Students should learn how to investigate the nature of the space where they are sharing information and monitor the content and information about them that exists online. Also, students should be taught to participate online in ways that respect other people, including not sharing others' information without their consent.
7. Students should understand how to regulate the use of personal information. This seventh principle is about encouraging students to seek the *consent of parents* or a responsible adult, and know that they can refuse collections of personal data and monitor the information about them located online.
8. Students should be aware of their rights to delete information and control access to their information. The eighth principle focuses on students' rights to use technology to protect and secure their data. Examples include managing their settings and refusing geolocation, for example.
9. Students should develop critical and ethical digital citizenship skills. The final (ninth) principle is one of *digital citizenship* which includes learning to assess the reliability and credibility of information and identifying inappropriate or illegal content (IWG, 2016).

The Last Word—A Critical Stance

We encourage educators who are reading this chapter to discuss their level of comfort with the types of surveillance of youth and adolescents that seem increasingly similar to the surveillance methods used by the police in crime shows on television. Educators need to step back and consider carefully their level of comfort with presentations at schools that imply that parents are not capable or are too busy to help their children and adolescents discern safe and unsafe online spaces. While we would not question a specific type of internet

surveillance tool that is available to parents, we have questions about whether or not it is a good idea for parents to receive daily copies of young people's online transactions. We also want to raise questions about the rights of surveillance organizations to *out* students before they are ready to disclose their sexual orientation or gender preference to their families. We encourage educators not to accept forms of surveillance and curation of content uncritically.

> Educators need to step back and consider carefully their level of comfort with presentations at schools that imply that parents are not capable or are too busy to help their children and adolescents discern safe and unsafe online spaces.

Secondly, we find that there are holes in the protection net for students and teachers surrounding digital privacy. Teachers are encouraged by the pamphlets from the Information and Privacy Commissioner to gain consent before posting students' pictures and they are reminded to follow school district policies (Information & Privacy Commission, 2019). These guidelines, however, lack the specifics and the understandings implicit in the GPEN International Working Group Digital Education competencies (IWG, 2016) in areas such as digital permanence, digital footprint and the potential impact of data (re)combination on privacy and choice.

References

Accepting Schools Act, 2012, S.O. 2012, c. 5 – Bill 13. (2012, June 19). *Chapter 5: An act to amend the education act with respect to bullying and other matters*. Queen's Printer for Ontario. https://www.ontario.ca/laws/statute/s12005

Akyurt, E. (2020, March 30). *In a gray sweater on a laptop facemask* [Photograph]. Unsplash. https://unsplash.com/photos/hkd1xxzyQKw

Berryman, J. H. (1998, December). Duty of care. *Professionally Speaking, 1998*(4). https://professionallyspeaking.oct.ca/december_1998/duty.htm

Bourdages, G. (2017, December 11). *Person in front of red lights* [Photograph]. Unsplash. https://unsplash.com/photos/WDbuusPOnkM

Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act.' *First Monday, 16*(11), Article 3850. https://doi.org/10.5210/fm.v16i11.3850

Bradshaw, S., Harris, K., & Zeifman, H. (2013, July 22). Big data, big responsibilities: Recommendations to the office of the privacy commissioner on Canadian privacy rights in a digital age. *CIGI Junior Fellows Policy Brief, 8*, 1-9. https://www.cigionline.org/publications/big-data-big-responsibilities-recommendations-office-privacy-commissioner-canadian

Chen, B. (2015). Exploring the digital divide: The use of digital technologies in Ontario Public Schools. *Canadian Journal of Learning and Technology / La Revue Canadienne De l'Apprentissage Et De La Technologie, 41*(3), 1-23. https://doi.org/10.21432/T2KP6F

Children's Online Privacy Protection Act of 1998, 15 USC §6501: Definitions. (1998, October 21). http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

Dangerfield, K. (2018, March 28). *Facebook, Google and others are tracking you. Here's how to stop targeted ads*. Global News. https://globalnews.ca/news/4110311/how-to-stop-targeted-ads-facebook-googlebrowser

Electronic Privacy Information Center. (n.d.). *California S.B. 27, "Shine the Light" Law*. https://epic.org/privacy/profiling/sb27.html

Feathers, T. (2019, December 4). *Schools spy on kids to prevent shootings, but there's no evidence it works*. Vice. https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works

Federal Communications Commission. (2019, December 30). *Children's internet protection act (CIPA).* https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Fisk, N. W. (2016). *Framing internet safety – the governance of youth online*. MIT Press Ltd.

Flaherty, D. H. (2008, June). *Reflections on reform of the federal privacy act*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_ref_df/

Geary, J. (2012, April 23). *DoubleClick (Google): What is it and what does it do?.* The Guardian. https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring

Global Privacy Enforcement Network (GPEN). (2017, October). *GPEN Sweep 2017: User controls over personal information*. UK Information Commissioner's Office. http://www.astrid-online.it/static/upload/2017/2017-gpen-sweep—international-report1.pdf

Government of Canada. (2019, June 21). *Personal Information Protection and Electronic Documents Act (PIPEDA).* Justice Laws Website. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Government of Canada. (2021, June 22). *Canadian internet use survey, 2020*. The Daily. https://www150.statcan.gc.ca/n1/daily-quotidien/210622/dq210622b-eng.htm

Grant-Champan, H., Laird, E., Venzke, C. (2021, September 21). *Student activity monitoring software: Research insights and recommendations*. Center for Democracy and Technology. https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/

Hampson, R. (2017, December 29). *Scrolling apps* [Photograph]. Unsplash. https://unsplash.com/photos/cqFKhqv6Ong

Hankerson, D. L., Venzke, C., Laird, E., Grant-Chapman, H., & Thakur, D. (2022). *Online and observed: Student privacy implications of school-issued devices and student activity monitoring software*. Center for Democracy & Technology. https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/

Haskins, C. (2019, November 1). *Gaggle knows everything about teens and kids in school*. BuzzFeed. https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education

Hatmaker, T. (2021, July 7). *Google faces a major multi-state antitrust lawsuit over google play fees*. TechCrunch. https://techcrunch.com/2021/07/07/google-state-lawsuit-android-attorneys-general/

Hermant, B. (2018). *Free WiFi inside* [Photograph]. Unsplash. https://unsplash.com/photos/X0EtNWqMnq8

Hill, K. (2016, March 31). *How Target figured out a teen girl was pregnant before her father did*. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=5c44383a6668

Information and Privacy Commission for Ontario (2019). *Privacy and access to information in Ontario Schools: A guide for educators*. https://www.ipc.on.ca/wp-content/uploads/2019/01/fs-edu-privacy_access-guide-for-educators.pdf

International Working Group on Digital Education (IWG). (2016, October). *Personal data protection competency framework for school students*. International Conference of Privacy and Data Protection Commissioners. http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf

Levine, M. A. J. (2020, September 17). *Troubling Clouds: Gaps affecting privacy protection in British Columbia's K-12 education system*. BC Freedom of Information and Privacy Association. https://fipa.bc.ca/news-release-new-report-highlights-gaps-in-student-privacy-in-bcs-k-12-education-system/

Lohr, S. (2020, September 21). *This deal helped turn Google into an ad powerhouse. Is that a problem?*. New York Times. https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html

Madrigal, D. V. H., Venzke, C., Laird, E., Grant-Chapman, H., & Thakur, D. (2021, September 21). *Online and observed: Student privacy implications of school-issued devices and student activity monitoring software.* Center for Democracy & Technology. https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/

McLeod, J. (2020, June 12). *Double-double tracking: How Tim Hortons knows where you sleep, work and vacation*. Financial Post. https://financialpost.com/technology/tim-hortons-app-tracking-customers-intimate-data

Ministry of Education. (2020, August 13). Requirements for remote learning. *Policy/Program Memorandum 164*. https://www.ontario.ca/document/education-ontario-policy-and-program-direction/policyprogram-memorandum-164

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, R.S.O. 1990, c. M.56. (2021, April 19). Queen's Printer for Ontario. https://www.ontario.ca/laws/statute/90m56

NASA. (2015, December 26). *Connected world* [Photograph]. Unsplash. https://unsplash.com/photos/Q1p7bh3SHj8

Organization for Economic Co-operation and Development (OECD). (2021, January). Children in the digital environment: Revised typology of risks. *OECD Digital Economy Papers, 302*, 1-28. https://doi.org/10.1787/9b8f222e-en

Office of the Privacy Commissioner of Canada. (2021, August 13). *Guidelines for obtaining meaningful consent*. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#_seven

Office of the Privacy Commissioner of Canada (2022, January 24). *Data privacy week: A good time to think about protecting children's privacy online*. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220124/

Ohm, P. (2010, August). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57, 1701-1777. https://www.uclalawreview.org/pdf/57-6-3.pdf

Palfrey, J., Gasser, U., & Boyd, D. (2010, February 24). *Response to FCC notice of inquiry 09-94: "Empowering parents and protecting children in an evolving media landscape."* Berkman Klein Center for Internet & Society at Harvard University. https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Palfrey_Gasser_boyd_response_to_FCC_NOI_09-94_Feb2010.pdf

Robertson, L., & Corrigan, L. (2018). Do you know where your students are? Digital supervision policy in Ontario schools. *Journal of Systemics, Cybernetics and Informatics, 16*(2), 36-42. http://www.iiisci.org/journal/PDV/sci/pdfs/HB347PG18.pdf

Robertson, L., & Muirhead, W. J. (2020). Digital privacy in the mainstream of education. *Journal of Systemics, Cybernetics and Informatics, 16*(2), 118-125. http://www.iiisci.org/journal/pdv/sci/pdfs/IP099LL20.pdf

Solove, D. J. (2004). *Digital Person: Technology and privacy in the information age*. New York University Press. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications

Spiske, M. (2018, May 15). *Green binary code* [Photograph]. Unsplash. https://unsplash.com/photos/iar-afB0QQw

Steeves, V. (2014). *Young Canadians in a wired world, phase III: Life online*. MediaSmarts. http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf

Sweeney, L. (2004), Simple demographics often identify people uniquely. *Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000*. https://dataprivacylab.org/projects/identifiability/paper1.pdf

Telford, H. (2017, October 29). *Opinion: Public schools ask parents to sign away children's privacy rights*. Vancouver Sun. https://vancouversun.com/opinion/op-ed/opinion-public-schools-ask-parents-to-sign-away-childrens-privacy-rights/

Thompson, S. A., & Warzel. (2019, December 19). *Twelve Million phones, one dataset, zero privacy*. The New York Times: The Privacy Project. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Tullius, T. (2020, May 30). *A painting on a wall warning visitors about video surveillance* [Photograph]. Unsplash. https://unsplash.com/photos/4dKy7d3lkKM

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Venzke, C., & Laird, E. (2021, September 21). *CDT and Coalition of Education and civil rights advocates urge Congress to protect student privacy*. Center for Democracy & Technology. https://cdt.org/insights/cdt-and-coalition-of-education-and-civil-rights-advocates-urge-congress-to-protect-student-privacy/

Wojcicki, S. (2009, March 11). *Making ads more interesting*. Google Official Blog. https://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the New Frontier of Power*. Public Affairs.

Zuboff, S. (2020, June 24). *You are now remotely controlled: Surveillance capitalists control the science, and the scientists, the secrets and the truth*. The New York Times. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

3.

CASE STUDIES IN DIGITAL PRIVACY LEADERSHIP AND POLICY

Lorayne Robertson and Bill Muirhead

This chapter will help students to:

1. Structure a well-design case study on digital privacy in education.
2. Articulate why the case study method is an effective learning tool in graduate education.
3. Reflect critically on the case study they have selected to study.

Students taking the *Digital Privacy: Leadership and Policy* course are required to write a case study about digital privacy. When writing this case study, they are encouraged to base their digital privacy scenario in a context with which they are familiar, such as their individual experience or a known context. Students examine a problem or situation, suggest solutions and reflect on these solutions. The case study was a deliberate, pedagogical choice for this course for multiple reasons. In the next section, the authors explain the theory and the practice associated with case studies through seven elements:

1. Distributed learning
2. Continuous assessment
3. Active learning
4. Collaborative learning
5. Learning in a community of inquiry
6. Problem-based online learning
7. Reflective practice

Case Studies: A Deliberate Pedagogical Decision

1. **Distributed learning**: This is a deliberate element of course design that encourages students to circle back and examine key concepts frequently. As Carpenter (2020) explains, distributed learning (also called the spacing effect) promotes better learning because the learning opportunities are spaced apart and are more likely to catch students' attention. It can also link to multiple contextual clues. When students spread out their work, it has a direct impact on how well they perform in the course (Eddy & Hogan, 2014). Distributed learning scaffolds the overall assignment into smaller assignments. The second assignment builds on the first, and so on. Students submit sections of the overall assignment for formative assessment. This allows students to obtain rich, detailed feedback at an early stage and helps to build confidence that they are *on the right track*. The final assignment is a culmination, demonstrating summative learning throughout the course.
2. **Continuous assessment**: One of the affordances of information and communication technologies is the means to provide rich feedback in multiple formats including providing digital handwritten annotations to assignments, text comments within a document/assignment and video or voice feedback to assist students in exploring and completing assignments. Rich asynchronous feedback with synchronous discussions between the instructor and students that mimic the established *office hours* of old can create an environment where instructor and students are engaged in a context of learning together and exploring in unison.
3. **Active learning**: The pedagogical approach of active learning means that students are engaged in pursuing knowledge and co-constructing their learning (as opposed to passively acquiring learning provided by another source). Active learning is more engaging when the topic is relevant to the student and has a ring of authenticity because *this could happen* and this increases engagement. Key elements of active learning include collaboration, cooperation, and problem-solving. The pedagogy is student-centred, self-directed and self-reflective with the instructors as guides (In other words, the students are directing their learning and the instructor is a guide (Jonassen, 2011).
4. **Collaborative Learning**: This pedagogy, which requires individuals to work together toward a common goal has been widely researched (Laal, 2013). A critical element of collaboration is positive interdependence which means that each person in the group is responsible for their own learning and the overall learning of the team toward the common goal—in other words, no one succeeds unless everyone succeeds (Johnson et al., 1994). It does not mean that one or two persons assume the work for the others. It requires the individuals to take on responsibility for the social skills required, to allow and support the cognitive development of others in the group, and to participate in frequent group discussions toward the common goal (Laal, 2013).
5. **Learning in a Community of Inquiry**: The creation of an online community of inquiry requires more than providing a textbook or a series of lectures. The concept of a community of inquiry articulated by Garrison et al. (2001) is one that includes a commitment by all of the participants in the online

community to support collaborative engagement, academic discourse and critical reflection. The learning community works to build social presence—a climate of learning that is safe and includes open communication and affective elements. The second element is cognitive presence, which includes a sense of discovery, information exchange and application. There is also a teaching presence in online learning, setting up the course design and methods and building structures to support cognitive presence and social presence (Archer, 2009).

6. **Problem-based online learning**: Savin-Baden (2007) explains that problem-based learning (PBL) involves the study of complex, authentic scenarios that do not have one right answer but provide a focus for learning. Students work in groups to identify the problem and identify what they know or do not know about the problem. Using self-directed learning, they seek information and develop possible solutions. The act of generating solutions is a form of experimenting. Faculty act as facilitators, guiding from the side.

Note. Magnifying glass keyboard, by A. Olloweb, 2018.

7. **Reflection**: While some might argue that experience is the best teacher, others theorize that reflection plus experience is what is needed for learning to happen (Brookfield, 1995; Kreber, 2001; Larrivee, 2010). Many times, students will work through a case study or through problem-based learning and miss the essential element that has the potential to make the learning *stick* and this element is reflection.

Why Employ a Case Study in Graduate Education?

Case studies allow learners to examine a field of study when the context for practice in the field, in this case, digital privacy leadership and policy, is continuously changing and precariously complex. Both topics: privacy and education provide rich opportunities to theorize problems that are authentic (and sometimes ill-structured and messy) and try out solutions in a safe space. Case studies provide a means or method to:

- examine authentic problems,
- facilitate the examination of complex contexts,
- apply theory to practice in a safe space, and
- encourage deeper thinking while examining complex contexts.

The context of education is complex as is the topic of digital privacy in education. There is no such thing as

a typical day for educational leaders. Interactions will include opportunities to influence and be influenced by students, teachers, instructors, staff, other administration, parents, bus drivers, social workers, police officers, and community leaders, and this is by no means an exhaustive list.

Education is a part of society and education reflects what is happening in society. Education policies are part of larger policies, such as human rights legislation. Similarly, the anxieties of the larger society are reflected in education. In many ways, education is a reflection of the society (an open system) in which it exists and, as in society, decisions and policies are complex and multi-faceted.

Note. A glass ball in nature, by A. Anderson, 2020.

Writing a case study is like telling a story. Narrative inquiry has a long history both in and out of education and narratives help students to study the educational experience. According to Connelly and Clandinin (1994), "One theory in educational research holds that humans are storytelling organisms who, individually and socially, lead storied lives. Thus, the study of narrative is the study of the ways humans experience the world" (p. 2). When writing the case study, we recommend that students conceptualize this as telling a story and think about telling their story for an audience.

According to Gill (2011), a discussion case study is created to examine a topic or situation, present options, develop solutions and evaluate the solutions. Case studies are not written to identify the right and wrong solutions but *to examine, analyze and weigh complex and competing insights within a context* (Gill, 2011). The difference between a case and a case study is that a case is a real-life situation or as close to real-life as possible without breaching confidentiality, whereas a *case study* is an analysis of a situation (Gill & Mullarkey, 2015). A case study is also a clear pedagogical choice because it moves away from telling *a war story* about something that happened, to telling the story using a pedagogical design that encourages critical and reflective practice.

A case study creates an opportunity to safely explore problems in a safe context of storytelling. Cases can be thought of as thought experiments where the author can explore ideas through a recounting of actions and individual insights through their interaction with policies and problems. Problems can be described and situated within environments where solutions can be tested and explored without any real-world constraints. Exploring solutions to problems through a combination of fictional and everyday contexts creates spaces where solutions can be tested to the most confounding problems, and potential actions can be explored and planned for within a case. Case studies are a means for creativity where leadership, analysis, research, emerging and new technologies, method, subject matter, evidence and data can be purposefully manipulated creatively to explore the complexity of privacy and human behaviour.

Preparing Your Case Study Assignment

In this course, the case study assignment includes the following elements which are described below:

a) an executive summary;

b) description of the context/worksite and policy environment;

c) description of the people involved, their responsibilities, and accountability in the organization in addition to an organizational chart with respective reporting lines;

d) the problem and a variety of potential solutions;

e) critical reflection on the desired solution and decision to resolve the problem or conflict and the impact of the solution on the actors involved;

f) video presentation to describe the case study;

g) identification of the key discussion questions from the case and topics for critical reflection; and

h) the final paper which is a group paper. It should be approximately 2000 words excluding the reference list. Students should label which sections each group member contributed.

Here is an explanation of each of these segments of a case study:

Note. Private mail slot, by D. Topkin, 2016.

a) **Introduction**: This is a description of the case that should explain why this particular case study is compelling, important, or significant. Students will be encouraged to incorporate references into the introduction so that their scenario can be grounded in the literature or situated within gaps in the literature. A case study should have an overview (one page) that introduces the case and draws in or *hooks* the interest of the readers. The one-page case overview should do the following: 1) Introduce the key decision-maker or the protagonist in the case study by providing a name, this individual's role in the organization and a brief reference to the decision that needs to be made. 2) Include an overview of the case that provides some context, describing the educational institution, country or region, and when technology is involved, an overview of the technologies will be included in the context. 3) Incorporate an overview page that includes the decision that needs to be made and 4) explain the alternatives to the decision.

b) **Description of the context/worksite and policy environment:** The context of the case is presented in this section, which needs to cover the required information about the context working in

general from the broader context to the more specific elements of context. This will challenge students to consider how to explain a context so that others can situate themselves within the context for discussion. If technology is significant, the context description will include this within the context of the country or the region, the description of the particular school, college, or university setting. The policy environment is also significant, as the guidelines, laws or procedures for the school authority, district, institution and provincial or national authority may be important aspects of the context.

c) **Description of roles and reporting**: The people in the organizational unit within which the decision is to be made are presented in the third section, outlining the levels of responsibility and/or the stakeholder elements. This section should identify everyone who is involved in the case. If a chart is provided, a written explanation of the roles should also be provided. Again, this section should be fairly descriptive of all persons involved.

d) **The problem and a range of solutions**: Identifying the problem to be addressed in your case study is an important step. It is important here to distinguish between the causes of the problem, the symptoms of the problem and the actual problem. Working together, the case study group should identify any solutions that need to be made, identifying the nature of each solution, its importance, and the potential repercussions of that solution or decision. Alternative solutions should also be presented and explored fully, reflecting on each potential decision and its implications and potential impact. Within this section, students may call on related theories or models that might help with the consideration of this case.

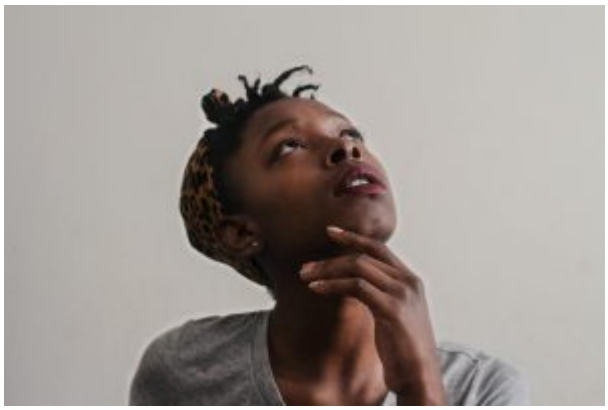
Note. Post-it board, J. Szczepanska, 2018.

e) **Critical reflection**: The closing section of the case study should present the final reflections of the decision-maker on the path that was chosen, the action plan or timeline, and anticipated outcomes. More importantly, the justification for the decision should be considered. When adult learners pause and re-consider the assumptions on which their learning has been built, they are engaging in *critical reflection*.

f) **Video presentation**: Students will prepare a digital version of the case study scenario and engage the class in academic discourse. Video presentations can often help to present a case in ways that reliance on text cannot. Video presentations may incorporate media types such as graphics, visual presentation of ideas, voice and video content that help others to understand the important context of a case study. As well, video allows both instructors and students to share cases in multiple learning environments. Case study videos can be created using voice-over PowerPoint, screen capture which incorporates audio elements as well as original video content and sets the stage, location and culture associated with the

case study. Those students who possess video editing skills may choose to create elaborate video content, while others may choose a less complex video format. The goal is to create a digital version of the case to *accompany the written case study* which can be presented in class.

g) **Reflection and discussion questions**: Each case study should include the discussion questions and key areas for reflection to encourage the class to engage in academic discourse.



Note. Woman looking up, by T. Lee, 2015.

h) **Final paper:** Groups should know that there is no single correct process for writing the group paper. In some groups, all of the writing is done together through a shared document. In others, writing is done in pairs. In others, one or two writers take the lead and others fill in with comments and reviews. What is key is that the group members should contribute more or less equally. The final paper should reflect the process of the group in problem-solving the case study. Use a spell and grammar checker. Sometimes groups do not leave enough time for revising. Fresh eyes: If possible, build in some time to set the paper aside and look at it.

	Length	Overview
Executive Summary of the Situation	1 page	• Provide an overview. Establish the significance • Introduce the key decision-maker(s) or write it in the 1st person as the protagonist • Draw in or hook in the reader
Context	1-2 pages	• Describe the region, worksite, and policy environment
People/ Organization	1-2 pages	• Describe the people, accountability aspects, stakeholders, organizational chart, and reporting lines
Problems and Solutions	1-2 pages	• Describe the type of decision needed, consider the alternatives. A rich case will have more than one right answer • Critically evaluate the possible solutions
Closing	1 page	• Reflect on the chosen decision and justify it. Reflect on the values on which it was predicated • Discuss the impact of the decision • Review the decision process and lessons learned
Discussion/ Reflection/ Lessons Learned	1 page	• Identify the discussion questions for this case study • Identify the key areas or topics for critical reflection

Note. Case study guidelines, by L. Robertson and B. Muirhead, 2017.

Case Studies as Learning

The concept of digital privacy in education provides rich opportunities to theorize problems and solutions to guide insights in authentic contexts. Above all, we need to keep in mind that a case study is a learning strategy that involves collaboration, communication, synthesis of information, creativity and imagination. Students who are writing case studies are using most of the levels of cognition in Bloom's taxonomy!

Case studies:

- facilitate the examination of complex contexts;
- help students apply theory to practice in a safe context;
- encourage deeper thinking;
- help students learn how to frame a problem;
- allow students to apply theory to practice;
- allow students to practice skills of short- and long-term decision-making;
- help students to appreciate multiple perspectives of multiple stakeholders;
- encourage consideration of the values and broader social issues surrounding cases;
- encourage critical reflection and reflective practice;
- allow students to practice writing and revision; and
- provide examples for other students to study and compare to similar stories.

At the present time, there is a shortage of case studies surrounding digital privacy and technology in education, indicating a gap in the field. The authors of this paper were unable to locate studies that examine learning in education leadership through case studies that include digital privacy, which may indicate that presently, there is a gap in the field. Similarly, there were no case studies located that were presented by students or to students for discussion using polysynchronous methods or digital contexts for their educational leadership studies. This is an area for further exploration where student-developed case studies could enrich the field. For example, educational leadership students can reflect on their learning when it is provided through the means of an engaging case study discussion and compare this with their learning from other methods such as problem-based online learning (Savin-Baden, 2007) and other forms of active, constructed online learning.

The authors of this paper were unable to locate studies that examine learning in education leadership through case studies that include digital privacy, which may indicate that presently there is a gap in the field.

A Few Final but Important Thoughts on Reflection

In the Digital Privacy: Leadership and Policy course, students are asked to provide their peers with reflective comments to improve their case studies. Peer feedback has been found to be one of the most powerful influences on learning but its impact can be both positive and negative; how the feedback is given is vitally important (Hattie & Timperley, 2007). Peer feedback is an active learning strategy. van Popta et al. (2016) analyzed the literature on peer feedback in online learning. They find that giving peer feedback benefits students by making them think more critically. It helps the peer-reviewers to improve their own work but

beyond that, helps students understand new concepts and build knowledge. Some studies show that peers compare their own work to that of their fellow students, and this internal feedback builds new knowledge. It is important to give peer feedback with explanations and examples so that the learner understands and benefits from the feedback. The process of giving good feedback builds students' writing skills (van Popta et al., 2016). In other words, peer feedback is a win-win proposition for more powerful learning.

Here are questions that students are asked to consider as the basis for their feedback on the Case Study presentations in the Digital Privacy: Leadership and Policy course:

1. Is the context for the case study realistic and explained well enough for the audience to grasp the key issues?
2. Does the context explain both the personnel involved and the policy environment?
3. From the description of the challenge of the case study, could the audience see opportunities for new policy directions or new actions?
4. Did the case study authors share the process they used for working on the case?
5. Did the case study authors incorporate multiple perspectives so that multiple opportunities and options were evident?
6. Did the case study authors allow for audience consideration, discussion and input on the potential solutions?
7. Was there evidence that the case study authors incorporated readings, policies and perspectives from the course?
8. Was this case study presentation an opportunity for the audience to learn and to reflect?
9. Do you have any other comments or recommendations for the presenter to help with the development of the final paper?

The use of case studies is, itself, an important teaching and learning strategy. Educators have many stories to tell based on their experiences. The process of a case study encourages students to examine the case study and work together to identify steps to work through a problem and weigh the potential outcomes. Educational problems are typically ill-structured (meaning messy), and no clear solutions are evident. The process of breaking down the problem into its small elements and analyzing the available resources and potential solutions is part of the learning. When working on a case study, students should be more concerned about developing strong problem-solving skills than *solving* the case. In fact, rather than settling on a solution early in the process, we encourage students to seek alternative solutions early in the process and develop their skills to determine why different solutions and resources might work in different contexts. The case study in this course has been constructed to encourage students to consider alternate perspectives of those who are impacted by the problem. Identifying alternatives and developing reflective questions are intended to assist students in both understanding different scenarios and beginning to weigh potential developments against other actions.

The reflective element of case studies is significant and important. Students need to push themselves to reflect on the pros and cons of solutions. They should expect that some of their previous assumptions can be challenged through this process. Cognitive dissonance is to be anticipated.

Pedagogies such as simulations, problem-based learning and case studies are intended to be safe learning environments where students can articulate their understandings and test out solutions without risk. Other

fields use simulations to train e.g., medical personnel. Today, we could not imagine training pilots without flight simulators. Having used case studies in the teaching of leadership and policy, we can attest to their value in encouraging critical, reflective practise without the pressure of seeking the perfect solution. We would argue that in a world characterized by change and complexity, understanding problem-solving processes and weighing the merits of different approaches to a problem are necessary skills.

References

Anderson, A. (2020, May 13). *A glass ball in nature* [Photograph]. Unsplash. https://unsplash.com/photos/HgZY0oYkpi8

Brookfield, S. (1995). *Becoming a critically reflective teacher*. Jossey-Bass Inc.

Carpenter, S. K. (2020, April). *Distributed practice or spacing effect*. Oxford Research Encyclopedia of Education. https://doi.org/10.1093/acrefore/9780190264093.013.859

Connelly, F. M., & Clandinin, D. J. (1990). Stories of experience and narrative inquiry. *Educational Researcher, 19*(5), 2-14. https://doi.org/10.2307/1176100

Eddy, S. L., & Hogan, K. A. (2014). Getting under the hood: How and for whom does increasing course structure work? *CBE—Life Sciences Education, 13*(3), 453–468. https://doi.org/10.1187/cbe.14-03-0050

Garrison, D. R., Anderson, T., & Archer, W. (2001). Critical thinking, cognitive presence, and computer conferencing in distance education. *American Journal of Distance Education, 15*(1), 7–23. https://doi.org/10.1080/08923640109527071

Gill, T. G. (2011). *Informing with the case method: A guide to case method research, writing, & facilitation*. Informing Science Press.

Gill, G., & Mullarkey, M. (2015). Taking a case method capstone course online: A comparative case study. *Journal of Information Technology Education: Research, 14*, 189-218. https://doi.org/10.28945/2171

Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of Educational Research, 77*(1), 1-112. https://doi.org/10.3102%2F003465430298487

Johnson, D. W., Johnson, R. T., & Holubec, E. J. (1994). *The new circles of learning: Cooperation in the classroom and school*. Association for Supervision and Curriculum Development.

Kreber, C. (2001). Learning experientially through case studies? A conceptual analysis. *Teaching in Higher Education, 6*(2), 217–228. https://doi.org/10.1080/13562510120045203

Laal, M. (2013, July 4). Collaborative learning; elements. *Procedia – Social and Behavioral Sciences. 83*, 814-818. https://www.sciencedirect.com/science/article/pii/S1877042813012202

Larrivee, B. (2000). Transforming teaching practice: Becoming the critically reflective teacher. *Reflective Practice, 1*(3), 293–307. https://doi.org/10.1080/713693162

Lee, T. (2015, November 02). *Woman looking up* [Photograph]. Unsplash. https://unsplash.com/photos/-wjk_SSqCE4

Olloweb, A. (2018, January 19). *Magnifying glass keyboard* [Photograph]. Unsplash. https://unsplash.com/photos/d9ILr-dbEdg

Robertson, L. & Muirhead, W. (2017). From War Stories to Critical Reflection: Learning through Case Studies in Graduate Leadership Courses. In, *Proceedings of the 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2017)* (pp. 335-339). http://www.iiis.org/CDs2017/CD2017Spring/papers/ZA068EW.pdf

Savin-Baden, M. (2007). *A practical guide to problem-based learning online*. Routledge.

Szczepanska, J. (2018, May 15). *Post-it board* [Photograph]. Unsplash. https://unsplash.com/photos/bjemWZcNF34

Topkin, D. (2016, March 30). *Private mailbox* [Photograph]. Unsplash. https://unsplash.com/photos/u5Zt-HoocrM

van Popta, E., Kral, M., Camp, G., Martens, R. L., & Simons, P. R. J. (2017). Exploring the value of peer feedback in online learning for the provider. *Educational Research Review, 20*, 24-34. https://doi.org/10.1016/j.edurev.2016.10.003

Walter, A. (2009). Beyond online discussions: Extending the community of inquiry framework to entire courses. *The Internet and Higher Education, 13*(1-2), 69. https://doi.org/https://doi.org/10.1016/j.iheduc.2009.10.005

4.

CRITICAL POLICY ANALYSIS

Lorayne Robertson and Bill Muirhead

This chapter will help students to:

1. Recognize digital privacy policies in different formats from different legislative sources.
2. Understand policy analysis as a changing landscape over time.
3. Analyze educational policies and identify policy gaps with respect to digital privacy.
4. Define and explore their understanding of the need for critical policy analysis.

Organization of the Chapter:

1. Defining Policy
2. Exploring Policy Analysis
3. Critical Policy Analysis

Fowler (2004) defines public policy as "the dynamic and value-laden process through which a political system handles a public problem" (p. 5).

Defining Policy

What is a policy?

- Intentions
- Rules
- Actions/Inaction
- Values

Note. Yellow arrow sign, by I. Pereira, 2017.

Many definitions of policy focus only on one aspect of the policy, rather than considering the context of the policy, the values that are reflected in the policy and how different groups may be affected differently by the policy. We encourage educational leaders to consider broader definitions of policy that include these other important considerations.

Policies can be defined informally as *the rules around here* or more formally as the regulations, laws or legislation that a public authority, such as a government or school district, passes in a response to an issue that in their view, requires a policy. Policies represent a decision or a series of decisions that someone or a group in authority has made. Pal (2010) defines a policy as a *public response to a problem*, but Fowler (2004) defines public policy as "the dynamic and value-laden process through which a political system defines a public problem. It includes a government's expressed intentions and official enactments as well as its consistent patterns of activity and inactivity" (p. 5).

Policies are not always planned as part of an agenda; they can happen when there is a convergence of issues.

Note. Ottawa freedom convoy, by V. Gagnon, 2022.

Policies are not always planned as part of an agenda; they can happen when there is a convergence of issues. Kingdon (1984) describes policy windows as opportunities that occur when regular policy development is disrupted. Here we use the example of the trucker blockade in Ottawa, Canada in February 2022 to explain Kingdon's policy streams and windows. In response to the blockade of the capital city and the bridges between the US and Canada by the truckers, there were multiple problems creating what Kingdon calls a problem stream. In response to a blockade, there was a public focus on the problem, creating a political stream. The proposed solutions to the problem were being suggested, creating a policy stream. Different groups wanted to see different results. As public opinion became energized over the issues created at the border crossings and in the capital city, there were multiple solutions proposed. As a result of the confluence of issues (problems) and solutions (policies), politically-motivated solutions begin to emerge. Streams change when leadership changes, creating more of a crisis or moving toward the resolution of a crisis. As Kingdon (1984) explains, this confluence of the streams opens a policy window.

In earlier times when policies were analyzed, there was an aim to have policies that were perfectly well

understood and with clearly delineated roles and results. Now, there is more of an agreement that policies need to consider multiple aspects of a policy, such as the values of members of society who are affected by the policy. This makes the study of policies rather cluttered and messy. Fowler (2004) studies policies in education, and she finds them to be nuanced and political. She reminds us that values shape policies. Deciding what constitutes the problem is also connected to values—take for example dress codes in schools. These dress codes can be highly value-laden and can be based on tradition and stereotypical norms. Even the decision that a dress code policy is necessary is also a value-leaden choice. Marshall argues that policies are more accurately defined as responses to problems that are identified by those who hold power (1999). For example, a decision whether or not to have a sexual harassment policy is a policy decision showing the values of those in charge (Marshall, 1999).

Exploring Policy Analysis

Yanow (2007) defines policy analysis as "a practice that entails the application of various research methods to policy issues and policy-making processes" (p. 111). Weimer and Vining (2017) define policy analysis as a "systematic comparison and evaluation of alternatives available to public actors for solving social problems" (p. 30). They note that there is a "fine line" between policy analysis and policy research which they define as a "synthesis of existing research and theory to predict consequences of alternative policies" (Weimer & Vining, 2017, p. 30). In the past, policy analysis focused on measurement based on stages of policy development, looking at how a policy was designed and comparing this to how it was implemented. This analysis was done to establish the quality of the policy. Policy analysts looked at the content of the policy, the policy design, the definition of the issue and the policy formulation, as well as its adoption and implementation. Policy analysis also looked at the impact or effects of a policy to ask whether the policy was fulfilling its stated role. Policy analysis used to be considered to be an objective process of analyzing the implementation of a policy. This analysis could include impact and efficiency evaluations such as cost-benefit comparisons. The measurement of the outcomes of a policy was done in an almost value-neutral way. More recently, policy has come to be understood as a more complex endeavour—or perhaps it could be argued that, presently, policy theorists have come to recognize more of the voices and different contexts for policy development and implementation.

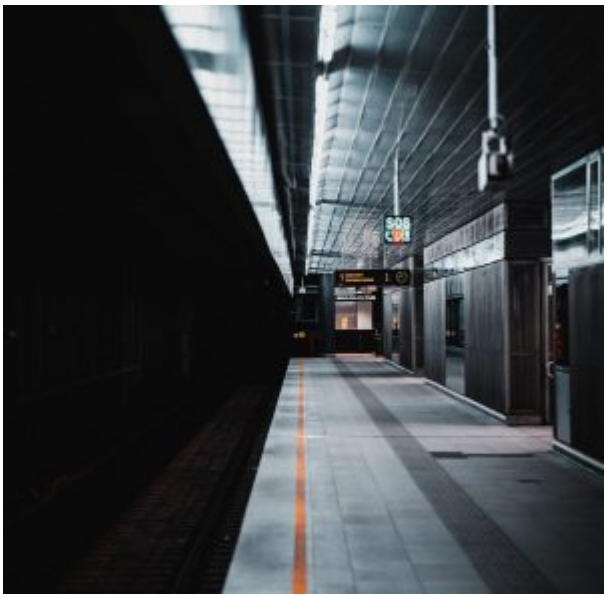
Policy actors: Ball et al., (2011) raise awareness of the role of policy actors; these are the persons who must make the policies work in schools. These policy actors receive the policies, and they are also responsible for enacting them or making them happen. Policy actors might be in charge of championing the policy and recruiting others to join the policy movement; conversely, policy actors in schools could be critics of the policy (Ball et al., 2011).

Policy contexts: Some policy theorists (e.g., Ball et al., 1994; Bowe et al., 1992) proposed that policies go through cycles in their development and implementation. Three different contexts which influence the design,

production and the effects of a policy were identified. In the context of influence, different interest groups can struggle over the construction of the policy and its discourses. In the context of policy text production, the policy analyst can ask which stakeholder groups were represented in the construction of the text, and who was excluded? And whose interests was the policy intended to serve? Multiple considerations fall under the context of practice, such as how well the policy is received, and to what degree the policy is open to interpretation (Bowe et al., 1992; Vidovich, 2001).

Policy trajectory: While some might argue that a policy remains the same once it has been written down and published, in fact, policies go through processes that can almost seem to take on a life of their own (Ball et al., 1994; Gale, 1999). Each policy undergoes its own journey or process as it is interpreted by those responsible for implementing or championing it. In the end, the policy is not just a text because it also contains actions (Gale, 1999). The text itself might also be incomplete. It may have contradictions, omissions or ambiguities (Bowe et al., 1992). Policies "land" into contexts of practice—Ball et al. (1994) sees policies as "textual interventions into practice" (p. 18). As policies are pronounced, they may pose problems for those in schools, and it cannot be assumed that every policy actor will interpret the policy in the same way. Policy enactment is affected by other factors such as understanding, cooperation, and resources (Ball et al., 1994).

Policy levers: There may be different responses to a policy such as acceptance, compliance, non-compliance and resistance. According to Steer et al. (2007), policy levers are the functional mechanisms that governments can use to ensure that policies are implemented. For example, the use of technology could be a learning expectation that is measured on the Ontario report card. If something is measured for the report card, it would ensure that it is taught; this is a policy lever.



Note. Train station, by A. Rainer, 2020.

Innovation-policy gap: Davis (2014) identified that the speed of technological progress created a gap between the innovators and policymakers stating that the pace of technological innovation was exceeding the pace of legislation or policy. He writes that, "policymakers are challenged to keep up with the latest developments in features, functionality, and business models. Meanwhile, technologists are innovating on a daily basis, often ignoring the potential impact that future legislation or policy might have on their endeavours" (Davis, 2014, p. 87). Davis also identified that other contexts such as social, political and cultural were shifting in addition to the technological, contributing to the innovation-policy gap.

Critical policy analysis

Theorists such as Marshall (1990) have argued that policy problems and analysis were traditionally addressed by the mainstream theorists who did not understand or acknowledge who was left out in policy discussions. Winton (2020) states, "Critical policy analysis refers to a body of research undertaken by scholars and activists in the pursuit of social justice" (p. vii). Diem et al. (2014) argue persuasively that education is changing and becoming more complex. Critical education theorists have emerged who are questioning taken-for-granted assumptions about education (e.g., Apple, 2012; Kincheloe, 2008). Diem and her colleagues challenge the traditional, positivist view of policy analysis which follows a sequence of steps (e.g., policy design, implementation and evaluation) designed toward measuring positive change. Instead, Diem et al. (2014) introduce research on an exciting new field: critical policy analysis. This more critical approach to policy analysis recognizes that policy problems in the past were defined and analyzed frequently by the mainstream (Marshall, 1990). As a result, Diem and her colleagues have really expanded how we think about policy analysis.

Diem et al., (2014) identify five fundamental concerns of critical policy theorists:

1. The difference between the rhetoric of the policy and the reality of policy in practice need to be examined.
2. The policy's roots and how they emerged. What issues was the policy intended to solve? Was its intent to maintain the dominant culture? How did the policy change over time? How did it become institutionalized?
3. Who were the winners and the losers as a result of a policy? Who gets what?
4. The effect of the policy on equality and privilege. How might a policy enforce or reproduce social inequality?
5. Do policy resistors engage in activism and participatory methods to build agency for policy change?

We agree that policy analysis is enabled through the design of frameworks. IN a discussion of policy processes, Sabatier (2007) describes policy frameworks as structures that consist of different descriptive categories or constructs; showing the relationships among them help to explain a phenomenon or what is happening. Such is the case with the Critical Policy Analysis Framework that we have designed.

We have created a policy analysis framework that guides critical policy analysis and also reflects the complexity of today's policy analysis. The development and use of a general framework helps to identify the elements and

relationships among these elements that one needs to consider for institutional analysis. Frameworks organize diagnostic and prescriptive inquiry. They provide the most general list of variables that should be used to analyze all types of institutional arrangements. Frameworks provide a metatheoretical language that can be used to compare theories. They attempt to identify the universal elements that any theory relevant to the same kind of phenomena would need to include. Many differences in surface reality can result from the way these variables combine or interact with one another. Thus, the elements contained in a framework help analysts generate the questions that need to be addressed when they first conduct an analysis.

Applying a Critical Policy Analysis Framework

Policy Influences	**Policy Texts**	**Policy Implementation**	**Policy Privileges** **(critical policy analysis)**
• Assumptions • Belief systems • Stance: traditional vs. contemporary	• Legislation: Acts, laws, Charters, Policy memos • Curriculum policies • Rhetoric or Discourse • Pronouncements e.g., media releases	• Policy trajectory • Policy actors • Policy levers • Policy contexts • Policy responses: (compliance, non-compliance)	• Policy history, complexity • Policy implications • Policy vacuums/ gaps • Rhetoric vs. reality • Policy alternatives and resistance
• Who has (traditional) power and voice in the policy process? • Who is missing?	• What is the stated public problem that the policy addresses?	• What are the intended and unintended repercussions?	• Policy privileges • Who has access? • Who has power? • Who owns the data? • Equity: Who benefits? Who is marginalized?

We would argue that a curriculum policy that does not teach about digital privacy or how to use social media in a manner that considers personal futures is one that has policy gaps and lacks relevance for today's students and instructors. Students need the support of both their parents and teachers to understand and navigate online. A curriculum policy can help students understand that *free* apps come with the cost of personal data and digital privacy. Students need to learn that their newsfeeds are curated and tailored to preferences that students

establish through their digital footprint. Students also need to know how their data becomes linked to their parents' accounts, and everyone needs to understand how their accounts become linked to their friends' and relatives' accounts through social media and to the information that is publicly available through voter lists and other public databases. Additionally, the school curriculum should acknowledge the realities of students' lived experiences online outside of school. Without this, there is a policy gap, and the curriculum becomes increasingly less relevant and unable to prepare students for work, life and personal safety in a digital era. We would describe the present Ontario curriculum as a policy desert with respect to curriculum expectations related to digital privacy.

An examination of the global bans on cellphones in schools reveals that educational authorities can use a discourse surrounding their technology that promotes and affirms school district decision-making surrounding technology, or they can use a discourse that inhibits innovation. For example, using the word *restriction* with respect to cell phone use is not enabling language. A policy discourse that describes technology as *exceptional* and something for which the province *grants permission* works against technology innovation and acceptance (Robertson, 2017).

Note. Child with phone silhouette, by A. Burden, 2017.

In August 2019, the Ontario Ministry of Education announced restrictions on the use of cell phones and other personal mobile devices in Ontario classrooms to take effect in November 2019. This was a missed opportunity for Ontario Education to support the many forms that technology-enabled learning takes in schools across the province (Robertson, 2017; Robertson et al., 2020).

Cell phone bans in general are problematic because these types of restrictions do not encourage schools and teachers to leverage the capacity of smartphones for learning. Most educators are aware that today's smartphones are hand-held computers—they have replaced cameras, audio recorders, scanners, navigation systems, personal trackers, bank machines and other devices. They also have maximum portability and functionality, and a cellphone's effectiveness for learning is close to a laptop. With hand-held devices, students can learn at any time and from anywhere. These technologies replace and augment student access to information and learning. The portability of hand-held devices makes education more accessible and more affordable.

Restricting cell phone use in schools is an equity issue. In the past decade of wireless substitution, many students are in homes that use phones for internet access. Cherwinski (2020) reports that 39% of persons with low income in Ontario do not have internet access, whereas only 1% of high-income earners in Ontario lack

internet access at home. American research finds similarly that families who rely on smartphones are more likely to be rural, non-white, and have less income compared to homes with multiple computers (Blumberg et al., 2016).

A critical policy analysis on a government ban on cell phone use then asks important questions such as, "Whose voices are present in this policy design and whose are missing?" and is an example of how critical policy analysis research works in the pursuit of social justice. The examination of cause and effect associated with a policy can lead to multiple perspectives which are often overlooked when developing a policy. Thus, critical policy analysis helps to establish a *360-degree* view of known and unknown consequences of policy outcomes.

References

Apple, M. W. (2012). *Education and power*. Routledge.

Ball, S. J., Goodson, I. F., & Maguire, M. (1994). What is Policy? Texts, trajectories and toolboxes. In S. J. Ball (Ed.), *Education reform: A critical and post-structural approach* (pp. 14-27). Open University Press.

Ball, S. J., Maguire, M., Braun, A., and Hoskins, K. (2011). Policy actors: Doing policy work in schools. *Discourse: Studies in the Cultural Politics of Education, 32*(4), 625-639. 10.1080/01596306.2011.601565

Blumberg, S. J., & Luke, J. V. (2016, December). *Wireless substitution: Early release of estimates from the national health interview survey, January–June 2016*. National Center for Health Statistics. https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201612.pdf

Bowe, R., Ball, S. J., and Gold, A. (1992). The policy process and the processes of policy. In R. Bowe, S. J. Ball, and A. Gold (Eds.), *Reforming education and changing schools: Case studies in policy sociology* (pp. 6-23). Routledge.

Burden, A. (2017, April 10). *Child with phone silhouette* [Photograph]. Unsplash. https://unsplash.com/photos/6jYoil2GhVk

Cherwinski, A. (2020, February 27). *The impact of Ontario's digital divide. AlphaPlus*. https://alphaplus.ca/download/the-impact-of-ontarios-digital-divide/

Davis, K. (2014). Bridging the innovation-policy gap. *The SAIS Review of International Affairs, 34*, 87-92. https://https://doi.org/10.1353/SAIS.2014.0015

Diem, S., Young, M. D., Welton, A. D., Mansfield, K. C., & Lee, P.-L. (2014). The intellectual landscape of critical policy analysis. *International Journal of Qualitative Studies in Education, 27*(9), 1068–1090. https://doi.org/10.1080/09518398.2014.916007

Fowler, F. C. (2004). *Policy studies for educational leaders: An introduction* (2nd ed.). Pearson.

Gagnon, V. (2022, January 29). *Ottawa freedom convoy* [Photograph]. Wikipedia Commons. https://commons.wikimedia.org/wiki/File:Convoi_de_la_libert%C3%A9_%C3%A0_Ottawa_02.jpg

Gale, T. (1999). Policy trajectories: Treading the discursive path of policy analysis. *Discourse: Studies in the Cultural Politics of Education, 20*(3), 393-407. https://doi.org/10.1080/0159630990200304

Kincheloe, J. L. (2005). *Critical pedagogy primer*. Peter Lang.

Kingdon, J. W. (1984). *Agendas, alternatives and public policies* (2nd ed.). HarperCollins.

Marshall, C. (1990). Educational policy dilemmas: Can we have control and quality and choice and democracy and equity?. In K. M. Borman, P. Swami, & L. D. Wagstaff, (Eds.), *Contemporary issues in U.S. education* (pp. 1-32). https://files.eric.ed.gov/fulltext/ED346543.pdf

Ministry of Ontario. (2019, August 29). *Ontario takes action to focus on learning*. Newsroom. https://news.ontario.ca/en/release/53505/ontario-takes-action-to-focus-on-learning

Ostrom, E. (2007). Institutional rational choice: An assessment of the institutional analysis and development framework. In P. Sabatier, (Ed.), *Theories of the policy process* (pp. 21-64). Routledge. https://doi.org/10.4324/9780367274689

Pal, L. A. (2010). *Beyond public policy analysis: Public issue management in turbulent times*. Nelson Education.

Pereira, I. (2017, April 26). *Yellow arrow sign* [Photograph]. Pexels. https://www.pexels.com/photo/yellow-arrow-led-signage-394377/

Rainer, A. (2020, January 22). *Train station* [Photograph]. Unsplash. https://unsplash.com/photos/0-UDsQcKlCg

Robertson, L. (2017). Assistive technologies at the point of instruction: barriers and possibilities. *Journal of Systemics, Informatics and Cybernetics, 15*(6), 18-24. http://www.iiisci.org/journal/CV$/sci/pdfs/IP028LL17.pdf

Robertson, L., Muirhead, B. & Corrigan, L. (2020). "Don't answer that!"- Cell phone restrictions in Ontario schools. In, *Proceedings of the 11th International Conference on Society and Information Technologies (ICSIT 2020)* (pp. 28-33). http://www.iiis.org/CDs2020/CD2020Spring/AuthorsH1.htm#

Sabatier, P. A. (2007). *Theories of the policy process*. Routledge. https://doi.org/10.4324/9780367274689

Steer, R., Spours, K., Hodgson, A., Finlay, I., Coffield, F., Edward, S., & Gregson, M. (2007). 'Modernisation' and the role of policy levers in the learning and skills sector. *Journal of Vocational Education and Training, 59*(2), 175-192. https://doi.org/10.1080/13636820701342574

Vidovich, L. (2001, December). A conceptual framework for analysis of education policy and practices. In W. Shilton, & R. Jeffery (Eds.), *Crossing borders: New frontiers in education research* (pp. 22). Australian Association for Educational Research. https://www.aare.edu.au/data/publications/2001/vid01267.pdf

Weimer, D. L., & Vining, A. R. (2017). *Policy analysis: Concepts and practice*. Routledge.

Winton, S. (2020). Introduction. In S. Winton, & G. Parekh (Eds.), *Critical perspectives on education policy and schools, families, and communities* (pp. vii-xvi). Information Age Publishing.

Yanow, D. (2007). Interpretation in policy analysis: On methods and practice. *Critical Policy Analysis, 1*(1), 110-122. https://doi.org/10.1080/19460171.2007.9518511

5.

POLICIES AND PRIVACY LEGISLATION

Heather Leatham

This chapter will assist students to be able to:

1. Understand and explain how the concept of privacy evolved to the present day.
2. Understand the strengths, weaknesses and gaps of the digital privacy policies in this chapter.

In this chapter, you will explore the evolution of privacy from common to international law and examine specific legislation that arose to protect the data that a digital world captures in increasing amounts. We'll also explore critical elements of Policies and Privacy Legislation as they relate to digital privacy broadly and in the context of education specifically, along with the relationships and gaps in the present North American policies. Further, the chapter affords opportunities to examine shared definitions and policies in Canada, the United States (U.S.), and Europe.

Note. Commodore PET 2001, by Rama, 2011.

Privacy as a notion and ultimately a concept requiring protection has long historical roots within European/Western law. By the 1970s, with the rise of smaller and more affordable home computers, the notion of privacy began to include protection in the new and expanding digital world that fits in the palm of our hand. Gülsoy (2015) describes digital privacy as "the right to privacy of users of digital media" (p. 338), which as a definition is broad. Jennifer Stoddart (2011), the former Privacy Commissioner of Canada, emphasized that as social media sites collect data, they have obligations only to collect what is necessary. Indeed, there is also an onus to inform the user of the intended data usage so that the consumer can make an informed decision (Stoddart, 2011). When a person decides to give access to their information, whether a person or an organization, they infer that their privacy will be protected just as it would be in a bricks-and-mortar operation (Robertson et al., 2019). In examining the policies and legislations that govern what can be collected and used, a better understanding of the current state of digital privacy in education emerges.

A Short History of Privacy

We can trace our understanding of privacy as a concept as far back as ancient Greek philosophy and through its modernization rooted in British Common Law (Holvast, 2009). Common examples include new technologies and personal letters, a protected asset against unwanted readers (Holvast, 2009). In North America, as early as the 15th century, New England colonists became compelled to enhance their personal privacy with the rise of *instantaneous* photography and the printing press. Indeed, the fancy new technologies likely inspired Warren and Brandeis's (1890) oft-cited and influential text The Right to Privacy (which helped shape US privacy legislation) in response to increased public access to officials' private lives.

Shortly after World War II, privacy legislation began noticeably expanding internationally. Two examples include Article 12 in the Universal Declaration of Human Rights (United Nations, 1948) and Article 8 in the initial European Convention for the Protection of Human Rights and Fundamental Freedoms (European Court of Human Rights, 2021). The articles are outlined in Figure 1 and are broad in scope but brief.

Note. Eleanor Roosevelt holding poster of the UDHR, by FDR Library, 2018.

Figure 1

Articles

Article 8, Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Equality and Human Rights Commission, 2021)

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (United Nations General Assembly, 1948)

Accompanying the rise of computers, we see the next generation of privacy legislation, starting in the Germany State of Hesse and the 1971 Data Protection Act, followed by Sweden's 1973 Data Act (Holvast, 2009). The United States then contributed four pieces of legislation within 14 years. Later in this chapter, we will look at the 1974 Family Educational Rights and Privacy Act (FERPA), the 1998 Children's Online Privacy Protection Act (COPPA), and the 2021 K-12 Cybersecurity Act. In Canada, privacy became nationally entrenched in 1982 with the Charter of Rights and Freedoms, the Privacy Act of 1985, and more recently the 2000 Personal Information Protection and Electronic Documents Act (PIPEDA). At the provincial level, most provinces have their own versions based on the 1990 Freedom of Information and Privacy Act (FIPPA), while at the third level of government, there is the 1990 Municipal Freedom of Information and Privacy Act (MFIPPA). All of which govern the collection and use of personally identifiable information (PII) through various government agencies.

Insights

- Sweden's Data Act is the first national legislation in the world on the topic.
- **What is PII**?: "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means" (U.S. Department of Labor, n.d., para. 1).

Building on the initial efforts, digital privacy has emerged as a realm of focus to sustain and uphold human rights such as freedom of expression (Ben-Hassine, 2021). The most recent and internationally enforced privacy legislation is from the European Union, the General Data Protection Regulation (GDPR), which has global implications. Businesses in other countries must adhere to the GDPR in order to conduct business with the European Union. Specifically in the context of collecting personal data and the new notion of *the right to be forgotten* which first appeared in 2014 after an EU Court of Justice decision.

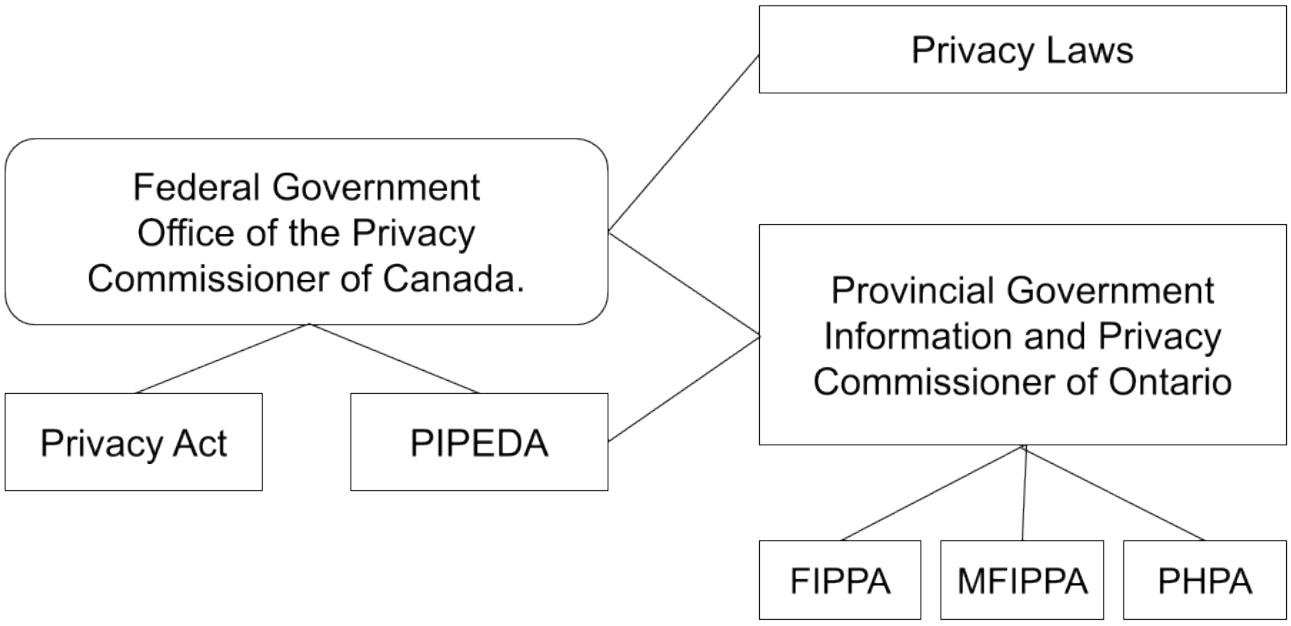
An Introduction to Government Privacy Acts

Privacy in Canada

As mentioned above, Canada's privacy legislation is primarily governed by the Privacy Act (c.P-21, 1985) and PIPEDA (2000). More recently is the Digital Privacy Act (c.32, 2015) which along with PIPEDA, governs activities related to private sector business and commercial activity.

Figure 2

Privacy legislation in Canada



Note. Privacy legislation in Canada, by H. Leatham, 2017.

None of the three aforementioned pieces of legislation are specific to education and minors (though MFIPPA governs education), a point that the Privacy Commissioner of Canada stated in a 2012 decision regarding the digital application Nexopia which was marketed primarily to the youth market.

Other privacy legislation occurs at the provincial/territorial level, of which the legislation from Ontario is used for the purposes of this chapter. There are two pieces of legislation in Ontario: FIPPA (c.F.31, 1990) and MFIPPA (1990) which govern the collection and use of personally identifiable information (PII), as well as defining what PII entails. Section 28 of MFIPPA defines PII and is outlined in Figure 3.

There have been some updates to Canadian legislation since the passing of the GDPR. According to the federal Privacy Commissioner, "Quebec tabled Bill 64 that would overhaul its private sector privacy law, B.C. announced the creation of a special committee to review its equivalent law, and in November, the federal government tabled the Digital Charter Implementation Act, 2020 as part of long-awaited PIPEDA reform" (Office of the Privacy Commissioner, 2020, p. 8). These are promising pieces of legislation though they still are aimed at commercial businesses for the most part.

Privacy in the United States

The United States recognized earlier than other countries the need to protect PII as it relates to minors starting with the *Family Educational Rights and Privacy Act* (FERPA, 1974). Even though computers at the time and digital records were not commonly being used, the collection of student data was still happening. Now

that much of the student information, from registration to assessment, is digital, FERPA continues to be applicable, as only the data collection methods have changed. Interestingly, FERPA allows for the disclosure of PII "to organizations conducting studies for, or on behalf of, the school, in order to: a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction" (sec. 99.31(a)(6)). With more instruction and classroom assessments using digital tools, if a school district has a contract with a company, Google for example, then the company has access to the metadata produced by students whenever they are using the digital tools, including PII (Privacy Technical Assistance Center, 2014).

FERPA has four exceptions to the disclosure of PII that are applicable to online tools (see sec. 99.31(a)(1)(i)). In order for the exception around being a provider to be valid, the onus is on the school or the district to determine if the provider is a *legitimate educational interest*. In some cases, the terms of service form from the provider may encompass all the legal requirements the provider must and will be following (Leatham, 2017).

Between 1984 and 1997, there was a large increase in computer usage both at home and at school in the United States. US households with home computers jumped from 8.2% in 1984 to 36.6% in 1997 (Infoplease, n.d.), with Infoplease (2017) reporting that there were 63.5 students for every one computer in public schools during the 1984-85 school year. However, the ratio changed to 6.3 students for every computer by the 1997-98 school year (Infoplease, 2017), representing a ten-fold increase in the computer to student ratio over 13 years. With this increase of computer availability and prevalence in both education and home settings, the US passed the Children's Online Privacy Protection Act (COPPA, 1998). COPPA specifically addresses the online privacy of children under 13 years of age, and it requires parents/guardians to give their consent to the use of both websites and digital applications.

The GDPR also has an age requirement under Article 6 but as of 16 years (GDPR, 2016), while Canada has no age specification in any privacy laws. According to the Federal Trade Commission (FTC), COPPA "imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age" (FTC, Part 312, 1998). COPPA requires companies to follow five specific rules in order to comply. As mentioned above, this includes:

- obtaining parental consent,
- posting a privacy policy,
- having a notice for parents,
- protecting the integrity of the collected PII, and
- allowing parents to review, revoke consent and delete their child's information (COPPA, sec. 312.6).

The newest American law, the *K-12 Cybersecurity Act* (2021) requires a study of cybersecurity risks specific to schools and school districts. The law focuses on student and staff records and a review of the information

systems *owned, leased, or relied upon* using guidelines created by the Cybersecurity and Infrastructure Security Agency. The results of the studies will be published on the Department of Homeland Security's website and be completed within a short time frame of 120 days from the enactment of the Act. President Biden (2021), in signing the Act into law, remarked that it "highlights the significance of protecting the sensitive information maintained by schools across the country," and "is an important step forward to meeting the continuing threat posed by criminals, malicious actors, and adversaries in cyberspace" (para 2).

Privacy in the European Union

Though there were privacy laws enacted in the 1970s in Europe, it was not until 1995 that a pan-European law was enacted, the European Data Protection Directive to protect the privacy of all EU citizens. After its publication, member states were to create their own laws to comply with the minimum of data protection it outlined (Wolford, n.d.). In 2016, an update was established when the EU decided "to harmonize data privacy laws across Europe" (Wolford, n.d.) and passed the *General Data Protection Regulation* (GDPR) which came into force in all EU countries in May 2018. The reason this law is mentioned here is that the legislation applies to any data of a European citizen whether that data is collected within Europe or not. Article 3 states, "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (GDPR, 2016). As a result, all companies outside of Europe have to comply with the GDPR and amend their privacy practices in order to continue doing business within the EU. Though not specific to education, the GDPR contains an age provision as mentioned earlier in this chapter. The reality that digital apps in other countries must comply is protection for students' PII.

The Challenge of Defining PII

PII, or Personal Data in other regions, is currently a pervasive concept but lacks a unified definition (Parkinson, 2018). While some identifiers overlap in the four Acts such as *age, geolocation, health,* and *phone numbers,* the only one that is common is *name*. Even using the term identifier poses challenges as Acts such as GDPR offer vague insights while FERPA moves to include scaffolded insights that include indirect identifiers. Further, some terms have multiple meanings, such as the concept of *personal self* in digital environments

Note. Code on a computer monitor, by M. Spiske, 2017.

(Parkinson et al., 2017). As a result, the globally interconnected but unique Acts foster disconnects and miscommunication as different parties may interpret information differently simply by following their localized guidelines.

Canadian Policy Gaps and Education

Building on the broad approaches to PII within North America and the European Union outlined above, I propose that it is critical to increase our focus on educational environments, specifically K-12-aged students in Canada. Pal (2010) defines public policy as "a course of action or inaction chosen by public authorities to address a given problem or interrelated set of problems" (p.35). However, public policy "is made in response to some sort of problem that requires attention" (Birkland, 2014, p. 8). The GDPR is currently a strong example of an actionable and focused response to diverse problems across the European Union, especially as it can extend into the digital classroom more readily.

The obvious Canadian policy gaps in the protection of student PII have been previously noted in Chapter 2. Still, the lack of digital privacy protection for minors within Ontario and Canada is worrisome. As the COVID pandemic shift to online learning has increased the use of digital platforms, decision-makers are seeking guidance on best-practice for online platforms in the context of the current privacy laws. Yet, the lack of guidance for school boards in this digital strategy continues to put the onus on individual boards and districts to develop scattered strategies instead of building on one cohesive, provincial-wide approach. Updating the MFIPPA to include a digital landscape could be a strong starting point, at the very least.

Hopefully, we will be afforded an opportunity to make some progress shortly, as the Privacy Commissioner of Ontario (OPC, 2020) has stated an intent to,

> Flesh out more details of its digital and data strategy Building a Digital Ontario, which includes plans to accelerate open data initiatives, create a new provincial data authority, and develop an online portal and other educational guidance on online data rights. (p. 11)

References

Ben-Hassine, W. (2021, December 18). *Government policy for the internet must be rights-based and user-centred*. United Nations. https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred

Biden, J. (2021, October 08). *Statement of President Joe Biden on signing the K-12 cybersecurity act into law*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/08/statement-of-president-joe-biden-on-signing-the-k-12-cybersecurity-act-into-law/

Birkland, T. A. (2011). *An introduction to the policy process: Theories, concepts, and models of public policy making* (3rd ed.). M.E. Sharpe.

Equality and Human Rights Commission. (2021, June 24). *Article 8: Respect for your private and family life*. https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

European Court of Human Rights. (2021, August). *European convention on human rights: A living instrument*. Council of Europe. https://echr.coe.int/Documents/Convention_Instrument_ENG.pdf

FDR Presidential Library & Museum. (2018, June 06). *Eleanor Roosevelt holding poster of the Universal Declaration of Human Rights in 1949* [Photograph]. Flickr. https://www.flickr.com/photos/fdrlibrary/27758131387/

Federal Ministry of Justice. (2019). *Federal Data Protection Act of 30 June 2017. (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).* https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

f 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626). https://www.gesetze-im-internet.de/englisch_bdsg/

Gülsoy, T. Y. (2015). Advertising ethics in the social media age. In N. Taşkıran, & R. Yılmaz (Eds.), *Handbook of research on effective advertising strategies in the social media age* (pp. 321-338). IGI Global. https://doi.org/10.4018/978-1-4666-8125-5.ch018

Holvast, J. (2009). History of privacy. In V. Matyáš, S. Fischer-Hübner, D. Cvrček, & P. Švenda (Eds.), *The future of identity in the information society. privacy and identity 2008. IFIP advances in information and communication technology, 298* (pp. 13-42). Springer. https://doi.org/10.1007/978-3-642-03315-5_2

Infoplease. (n.d.). *U.S. Households with Computers and Internet Use, 1984? 2014*. https://www.infoplease.com/math-science/computers-internet/us-households-with-computers-and-internet-use-1984-2014

Infoplease. (2017, February 28). *Computers in public schools*. https://www.infoplease.com/askeds/computers-public-schools

Office of the Privacy Commissioner. (2020). *A year like no other: Championing access privacy in times of uncertainty*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2021/05/ar-2020-e.pdf

Leatham, H. (2017). *Digital privacy in the classroom: An analysis of the intent and realization of Ontario policy in context* [Master's dissertation, Ontario Tech University]. Mirage DSpace Repository. http://hdl.handle.net/10155/816

Pal, L. A. (2010). *Beyond public policy analysis: Public issue management in turbulent times* (4th ed.). Nelson Education.

Parkinson, B. (2018, April). *Personal data: Definition and access* [Doctoral dissertation, University of Southampton]. ePrints, University of Southampton Institutional Repository. https://eprints.soton.ac.uk/427140/

Parkinson, B., Millard, D. E., O'Hara, K., & Giordano, R. (2018). The digitally extended self: A lexicological analysis of personal data. *Journal of Information Science, 44*(4), 552–565. https://doi.org/10.1177/0165551517706233

Privacy Technical Assistance Center. (2014, February). *Protecting student privacy while using online educational services: Requirements and best practices*. U.S. Department of Education. https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

Rama. (2011, October 26). *Commodore PET 2001* [Photograph]. Wikipedia Commons. https://en.wikipedia.org/wiki/File:Commodore_2001_Series-IMG_0448b.jpg

Robertson, L. P., Leatham, H., Robertson, J., & Muirhead, B. (2019). Digital privacy across borders: Canadian and American perspectives. In, A. Blackburn, I. L., Chen, & R. Pfeffer (Eds.), *Emerging trends in cyberethics and education* (pp. 234-258). IGI Global. https://doi.org/10.4018/978-1-5225-5933-7.ch011

Spiske, M. (2017, February 14). *Code on a computer monitor* [Photograph]. Unsplash. https://unsplash.com/photos/Skf7HxARcoc

Stoddart, J. (2010). Privacy in the era of social networking: Legal obligations of social media sites. *Saskatchewan Law Review, 74*, Article 263. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sasklr74&div=20&id=&page=

United Nations General Assembly. (1948). *Universal declaration of human rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United States Department of Labor. (n.d.). *Guidance on the protection of Personal Identifiable Information*. https://www.dol.gov/general/ppii

Warren. S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220. https://doi.org/1321160

Wolford, B. (n.d.). *What is GDPR, the EU's new data protection law?*. GDPR. https://gdpr.eu/what-is-gdpr/

6.

THE PRIVACY PARADOX: PRESENT AND FUTURE

Lorayne Robertson

This chapter will assist students to be able to:

1. Understand how research has informed current understandings of the privacy paradox.
2. Explain how research is informing policy designers for ways to address the privacy paradox, including privacy by design.
3. Apply understandings from this chapter to educate others on the implications of the privacy paradox and the need for privacy by design.

Defining the Privacy Paradox

A paradox is a logically self-contradictory statement or a statement that runs contrary to one's expectation. It is a statement that, despite apparently valid reasoning from true premises, leads to a seemingly self-contradictory or a logically unacceptable conclusion.

(Wikipedia, 2022)

The privacy paradox is a conceptual model that attempts to capture the trade-off between convenience and privacy. While studies indicate that people want to guard their personal information closely (Antón et al., 2010), the ease with which customers can bypass the terms of service (TOS) or privacy policies in online applications is part of the puzzle of privacy protection in the digital age that challenges research to establish its contributing factors. It is in the best interest of the economy to maintain consumer trust in online commerce by protecting digital privacy.

At times, it appears that innovation is eroding the protection of privacy. Increasingly, one can argue that the ability NOT to be tracked or observed today is elusive. There is surveillance tracking shopping in stores, observing the patterns that shoppers take in the stores and their choices as consumers. Many new applications are designed to provide a service but simultaneously erode solitude and privacy through tracking mechanisms. Vehicles and devices have GPS trackers; wearables track fitness levels, activities and location. The Internet of things (IoT), which includes home appliances, tracks and exchanges personal data about the lives of persons in the home. While people are on mobile devices constantly communicating with each other, online services are tracking them. Given this level of surveillance, one could not blame the average citizen if they concluded that loss of privacy is inevitable. It may also be the case, however, that given the overall digital privacy picture in Canada, privacy protection policies and TOS are poorly understood and under-subscribed to by the users and deliberately not explained well by the vendors.

Note. Home shopping, by I. Miske, 2017.

One contribution to the general erosion of privacy are trends such as is the significant increase in online professional and social networking. At times, participation in professional sites that share information about your personhood is encouraged by employers. According to Antón et al. (2010), LinkedIn, for example, garnered some 33 million users, just in its first five years. Facebook, which is a global social networking site, had 2.9 billion users at the close of 2021 (Statista.com). The global pandemic also contributed by moving much of Canadian retail online. Online shopping is very popular in Canada with more than 28.1 million Canadians making purchases online and a reported 3.3 billion Canadian dollars in monthly retail e-commerce sales (Coppola, 2022). Many of these sites require customers to provide their email, allowing the retailer to tailor and personalize advertising to them.

At the same time, unconnected to commercial use, newer technologies are emerging that have privacy implications. One example is body-worn cameras employed by police services, designed to protect both the public and the officers yet they also surveil the general public. Another recent innovation is virtual health care. There has been a proliferation of apps provided recently where patients can download and track their health history from the hospital or check the results of their latest tests online. In addition, since the onset of the pandemic, virtual health care visits have become the norm. In Ontario, there is an online health service that provides medical advice 24/7. Each of these emergent affordances should be reviewed for the privacy and security risks that are associated with them, particularly in light of frequently-reported data breaches in other sectors.

While digital technologies offer more affordances than ever before, one of the risks connected to these affordances is privacy. In this chapter, we explore the digital privacy paradox which occurs when concerns

about privacy are weighed against convenience. This paradox has not always existed—it is more of a development that has emerged over the past 15 years. Powell (2020) reports that Zuboff explained to the Harvard Gazette that only 1% of global information was digitized in 1986. By the year 2000, this had increased to 25 percent. By 2007, the amount of information digitized globally was 97% and this came to represent the tipping point. Today most information is digital (Powell, 2020). Table 1 provides some examples of the privacy paradox enacted in daily life and in education.

Table 1

Gains Versus Privacy Tradeoff

Scenario	Gains	Tradeoff
It is 11 pm, and you are on the highway in an unfamiliar setting. You need a hotel, so you download a hotel cost comparison app. The privacy agreement is 17 pages long, so you click through to get to the app without reading the agreement.	Convenience, Safety, Shelter	Privacy
As a teacher, you need an app to provide visualization for a math lesson. It will not let you add a class list of pseudonyms to participate on the app. Every student has to provide their personal email or their parents' email in order to join.	Providing the best educational experience possible	Students' and parents' private information may be compromised for third-party providers
As a parent, you hear that all students in the class are using a cloud-based data sharing app for writing schoolwork, but you have a concern that your child's data will be in the cloud.	Your child needs to be connected in school and part of the class	Students' and parents' private information may be compromised for third-party providers
You want to collect points, so you download the loyalty app to your favourite coffee shop.	Loyalty rewards, they know your order, they prepare your order in advance	Privacy is compromised as this app and its related apps track your location constantly
Big data employs AI and algorithms to mine the data so that advertising can be targeted directly to a classification of customers who are in a similar demographic. This provides a competitive edge to the company and supports the digital economy	Personalized service, less time to load in the information each time	Your personal information is sold and shared with third parties, risk of privacy violations, breeches, identity theft

Solove (2020) writes that the privacy paradox, which was identified more than 20 years ago as an "inconsistency between stated privacy attitudes and people's behaviour" (p. 4) is not a paradox but is, instead, an illusion and a myth. He sees futility in the concept of privacy self-management, and he states,

> Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively. The best people can do is manage their privacy haphazardly. People can't learn enough about privacy risks to make informed decisions about their privacy. (p.3)

Further, Solove (2020) explores various studies that have established evidence of the paradox between people's intentions online and their actions. He acknowledges the role that technology has played in designing consent stating,

> The Internet makes it easier for people to share information without the normal elements that can make them fully comprehend the consequences. If people were put in a packed auditorium, would they say the same things they say online? Most likely not. When people post online, they don't see hundreds of faces staring at them. (p. 15)

Solove recommends that privacy regulation should be strengthened so that the laws do not rely on individuals managing their own privacy. His argument is that privacy regulation, "should focus on regulating the architecture that structures the way information is used, maintained, and transferred" (Solove, 2020, p. 3).

In the section that follows, some of the emerging research on the privacy paradox is outlined, providing more insights on whether the most promising solutions are leaning toward increased legislation or consumer empowerment.

Understanding the Privacy Paradox

Recognizing that the privacy paradox is an established construct, one approach would be to look for solutions to address it or change aspects of it so that there is more compliance and less of a paradox. Some might look for top-down approaches to protect digital privacy, in the form of stronger or more specific policy (laws and legislation); others might seek bottom-up solutions that educate the consumer and encourage them to exercise care to protect their privacy. There is general agreement that fair information practices should offer notice to inform users when information is being collected and for what purpose; and choice about whether or not the information is shared (See PIPEDA in Chapter 2.). There is also a recognition that the TOS are generally not that helpful in protecting privacy (e.g., Awad & Krishnan, 2006; Massara et al., 2020).

Note. Digital thoughts, by Prostock-Studio, 2020.

Researchers disagree on the approach forward. The approach that some researchers have taken is to investigate consumers' choices and thought processes when faced with TOS or a privacy policy in order to download or use an application. What has emerged in the flurry of research surrounding digital privacy in the present era, is the understanding that the privacy paradox is not unidimensional, and there are multiple factors to be considered.

Obar and Aeldorf-Hirsch (2018) claim that the clickthrough agreement (they call this clickwrap) discourages and thwarts the critical inquiry that is central to deciding notice and choice; this results in supporting business. They define clickwrap as,

> A digital prompt that enables the user to provide or withhold their consent to a policy or set of policies by clicking a button, checking a box, or completing some other digitally mediated action suggesting "I agree" or "I don't agree." (p.3)

The policies may not be written out, instead, there may be a link to the privacy policies or TOS. In other words, a clickthrough policy appears to be deliberately designed to discourage more critical choices. They theorize that, while the length and complexity of policies impact user engagement with them, this "does not tell the whole story" (p. 3). One factor may be resignation that the consumer is powerless to make substantive changes. A more deliberate strategy suggested is that social media takes advantage of the clickthrough in order to connect users to social media services as quickly as possible in order to monetize their involvement as quickly as possible. Advertisers want to avoid controversy, disagreement and critical review of the policies in order to keep consumers in a "buying mood" (p. 6). Other factors may come into play, such as using the smaller icons for the privacy policy or other similar efforts to discourage users to engage in the consent process fully (Obar & Aeldorf-Hirsch, 2018).

Obar and Oeldorf-Hirsch (2020) asked adults to join a fictitious social networking site. They observed how the digital clients approached the privacy policies and TOS agreements. The result was that 74% skipped the privacy policy using the clickthrough option. If they did not select the clickthrough option and *read* the privacy policy, the average reading time spent on the privacy policy was 73 seconds. Most (97%) agreed to the privacy policy. In a surprising finding, 93% agreed to the TOS even though the TOS had *gotcha* clauses indicating that data would be shared with the NSA and participants would provide their first-born child as payment. The researchers concluded that information overload is a significant negative predictor for skimming rather than reading the TOS, and participants view policies as a nuisance" (Obar & Aeldorf-Hirsch, 2020).

Wang et al. (2021) see the paradox as the competing interests of the economic realities of the need for big data to support e-commerce and the privacy needs of individuals, (which they see as a psychological need). They explore an additional paradox, which is the one between attitudes toward privacy and privacy-protective behaviours. Their research indicates that online users also have peer privacy concerns, which they describe as "the general feeling of being unable to maintain functional personal boundaries in online activities as a result of the behaviours of online peers" (p. 544).

Another privacy paradox explained by Massara et al. (2021) is that, while Europeans indicated that they were concerned about privacy, it seemed that it would follow that consumers would not choose Google and Facebook, who had been sanctioned for privacy violations. The paradox was that, instead of discouraging online participants when violations occurred, the Google search engine had a 90% market share in Europe. The reported results were similar for YouTube and Facebook in the US. As a result, Massara et al. (2021) investigated whether consumer consciousness of the risks associated with digital privacy would be sufficient to change their behaviours.

Massara et al. (2021) find that perception of risk is unlikely to impact consumer consent. What is more likely to impact consent to disclosure are the perceived benefits and familiarity with the site or organization collecting the data. More importantly, Massara and colleagues' research shows that "the privacy paradox is not a monolithic construct but one that is composed of several possible facets" (p. 1821). This research team concludes that the relevance of the variables they have identified regarding consent suggests that companies should facilitate tools for customer choice and facilitate the empowerment of consumers to make informed decisions—even helping consumers to understand the impact of their choices. They recommend the kind of protections established in Europe such as providing limits on data processing, allowing for the withdrawal of consent and also what is known as *the right to be forgotten* in the European privacy legislation (Massara et al., 2021). They find that this matches Solove's (2020) argument that people make decisions about risk in specific contexts while their views about privacy are more general.

At this point in time, there are arguments both for top-down solutions through policies and for bottom-up solutions aimed at increasing consumer empowerment for digital privacy choices. When engaging with European online publishers recently, this author has noted that the right to consent to cookies is explained clearly on their website. The user has clear choices and buttons to click with respect to choices surrounding disclosure of information, consent to be on an email list, or disclosure of personal information to third parties. This level of consumer clarity for notice and choice, if practiced more generally, has the potential to erode the perception of a privacy paradox.

The Privacy Paradox in Education

The paradox of privacy occurs when security is weighed against convenience. We consider this paradox in light of the increasing use of technology by teachers and school districts.

(Robertson & Muirhead, 2019)

There is a growing awareness that technology is helpful to students (Pierce & Cleary, 2016). European research shows that the use of technology in schools benefits student learning, impacts student motivation in a positive way, promotes more student-centred learning and increases the number of teaching and learning strategies used. There is also growing awareness that Information and Communication Technologies (ICTs) are helpful to students in schools (Balanskat et al., 2006). Similarly, the American government notes that technology use in education increases tools for learning, expands course offerings, accelerates student learning and also increases motivation and engagement (US Department of Education, n.d.). Some research notes a positive impact on student learning outcomes (Greaves et al., 2012).

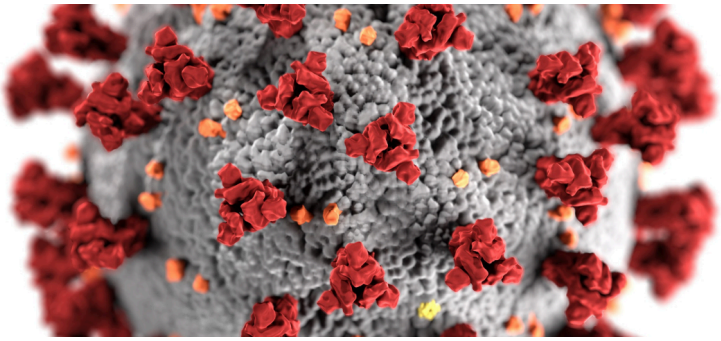
Note. Cable connection, by L. Kienle, 2020.

While the cost of equipment negatively impacted the growth of technology use in schools, gradually schools introduced laptops and more portable devices into classrooms. When wireless technology became available, and bandwidth sufficiency issues were resolved, technology use in schools increased (Ahlfeld, 2017; Pierce & Cleary, 2016). As more research becomes available about increases in the use of technology during the pandemic, it will undoubtedly report an increase in the use of technology during emergency remote learning and similar shutdowns of in-person schooling. While internet usage continues to increase, the reality is that two-thirds of the children in the world do not have internet access at home (UNICEF, 2020) which has significantly impacted their education during the school closures from the pandemic. Similarly, 63% of youths ages 15-24 lack internet access globally (UNICEF, 2020).

In Canada, there is a different picture where 99% of Canadian students surveyed in one study have internet access (Steeves, 2014). Against this backdrop of ever-increasing online participation, digital privacy concerns emerge. Students and teachers who may employ click-through agreements to share their personal information may not be aware that they are leaving a digital footprint and that their information is tracked for purposes of creating lists to personalize the advertising and the news feeds that they receive. Students and teachers may not be aware that they are creating a digital dossier that provides data about themselves and their friends. Adults who supervise them may not know that these digital dossiers can be sold without alerting end-users (Robertson

et al., 2018) and that their online data has permanence. One issue is that youth may not be aware that their personal information is for sale. They may not be aware until there are consequences such as a denial of an application for work or for a loan.

The Privacy Paradox in the Age of Covid



Note. Virus, by CDC, 2020.

Schools have increasingly turned to large corporations to provide the *Learning Management Systems*, internal email and search engines to power students' learning. The advent of Chromebooks was a game-changer because students could work in the cloud and users could image their own devices. Within education, some research has indicated that teachers care about privacy, but they are also not aware of how to protect student privacy or how to encourage students to protect their privacy (Leatham, 2017; Leatham & Robertson, 2017).

During the period of emergency remote learning, where the pandemic resulted in rapid, emergency health decisions, government agents and school districts made decisions rapidly without consulting on the privacy aspects. For example, in Ontario, teachers were required to provide synchronous, online learning or hybrid learning, and there was insufficient time to research the privacy implications of young children appearing on the screens and showing their understanding of school-led learning with others watching. There are even risks for adults; Abrams (2020) reports that a hacker leaked the data from sites such as ProctorU, compromising the data of almost half a million participants. The abrupt shift to emergency online teaching has led to the purchase of outsourced applications before there was time to protect for privacy concerns. This emergency teaching may have led to the purchase of outsourced applications without comprehensive testing for privacy concerns. Germain (2020) describes the concern of a Canadian student who had to allow the scan of her face as well as her bedroom in order to take a test for her course at a Canadian University. Similarly, Abrams (2020) reports that a hacker released the data files at ProctorU which compromised the data of more than half a million test-takers. There were also concerns about equity issues for the proctoring services which were broadband width sensitive and involved persons watching students in their homes, leading to the Consumer Reports investigation (Germain, 2020).

Recognizing that Canadian children and youth are spending an increasing amount of time online both for socializing and for school purposes during the pandemic, Daniel Therrien, the Privacy Commissioner of Canada (Office of the Privacy Commissioner, 2022) co-sponsored a resolution on children's digital rights [PDF] that recognizes that the digital world provides opportunities to children but also can infringe on their rights such as the right to privacy. This global resolution affirms that the information posted about children can be collected and used by third parties and that those collecting data have a responsibility toward minors. The resolution stresses that children are particularly vulnerable and that children's online privacy is a priority. To that end, the resolution notes the need to raise awareness among caregivers and educators of the online commercial practices that could harm minors.

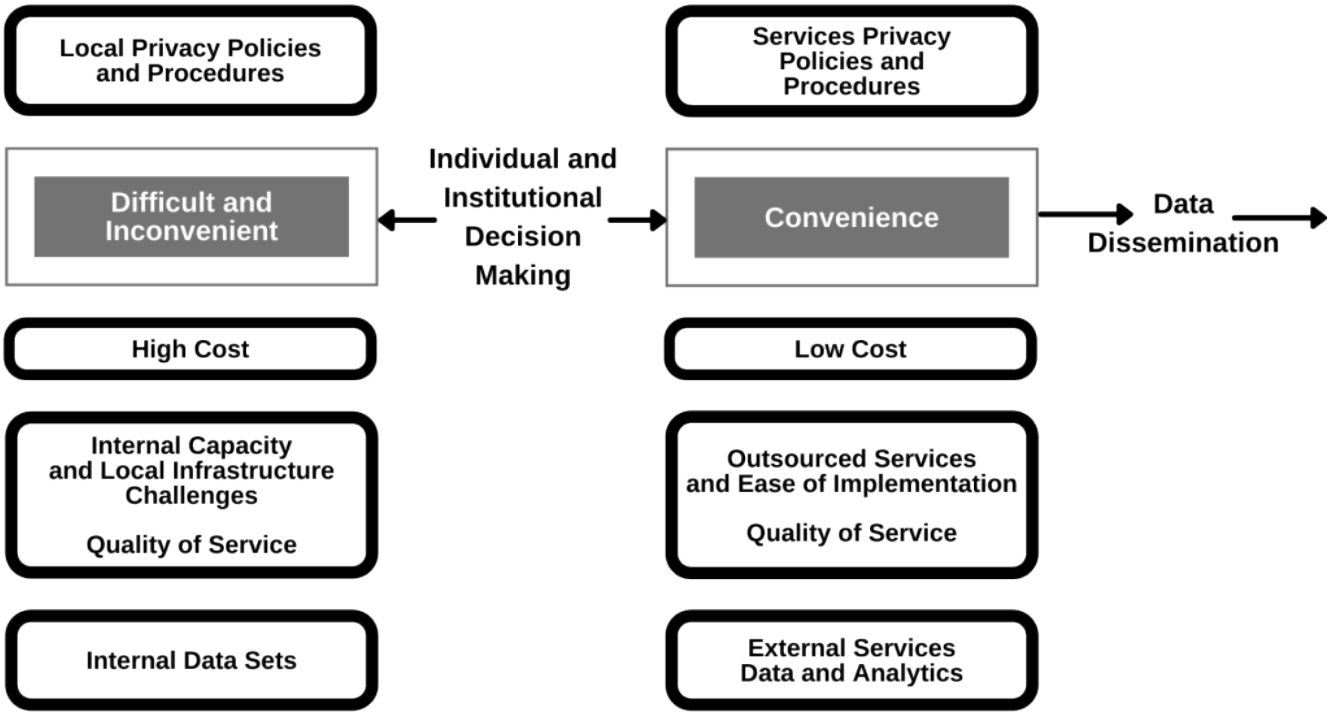
Robertson and Muirhead (2019) in describing the context for the digital privacy paradox in schools state,

> Privacy is often understood in terms of applications, infrastructure and risk associated with the use or unintended use of personal data. This orientation to "risk as the loss of data" omits decisions about what technologies, services and personal choices including beliefs, inform decisions made by individuals, groups or institutional services that collect data. While services are often seen as software and applications, increasingly, corporations are developing hybrid infrastructures that bundle services with specific hardware such as Google with Chrome Books and a G-Suite of applications for schools and students, or Apple with Ipads and iCloud or Amazon with their set of learning solutions including Amazon-Inspire, LMS and Amazon AWS (web services that run Cloud applications). (p. 31)

Robertson and Muirhead (2019) developed a framework for educational decisions that acknowledge the paradox between ease of use and decisions required for education. Recent data breaches and intrusions into corporate accounts have established some risks inherent in online participation and the erosion of trust concerning the external collection of personal data.

Figure 1.

Education and the Privacy Paradox



Privacy by Design

Dr. Ann Cavoukian, who was the Information and Privacy Commissioner for Ontario for three terms (17 years) created Privacy by Design and its 7 Foundational Principles (Cavoukian, 2011). There are seven principles in the concept of Privacy by Design and each one is just as important as the next. These principles are:

1. Proactive not Reactive/Preventative not Remedial.
2. Privacy as the Default.
3. Privacy Embedded into Design.
4. Full Functionality.
5. End-to-End Security.
6. Visibility and Transparency.
7. Respect for User Privacy.

Cavoukian (2019) in an interview compares Privacy by Design to a medical model that is interested in prevention before a privacy breach occurs. In her view, good privacy models promote creativity and it is in the best interest of businesses to promote good security models. Based on her experience, she advocates for a global framework of good privacy practices that include data portability (meaning that the customer can move personal data from one business to another) and the right to be forgotten. She advocates that having

privacy protected should be the default box in online choice—the app should give privacy automatically. This would take the onus off the user to protect their privacy. She sees benefits for business in following the seven principles. If businesses tell customers what they are doing and are transparent with them, a trusting relationship is more likely to develop and customers will be more likely to stay with the vendor.

Cavoukian (2019) also discusses how some of the current privacy risks have been created through newer devices that she describes as, *not ready for prime time* in her interview. Examples include digital assistants that listen in and broadcast personal conversations and the capture of mobile phone conversations with devices used by law enforcement such as the StingRay device; here the regulations to protect digital privacy have not caught up with the technology (Brend, 2016).

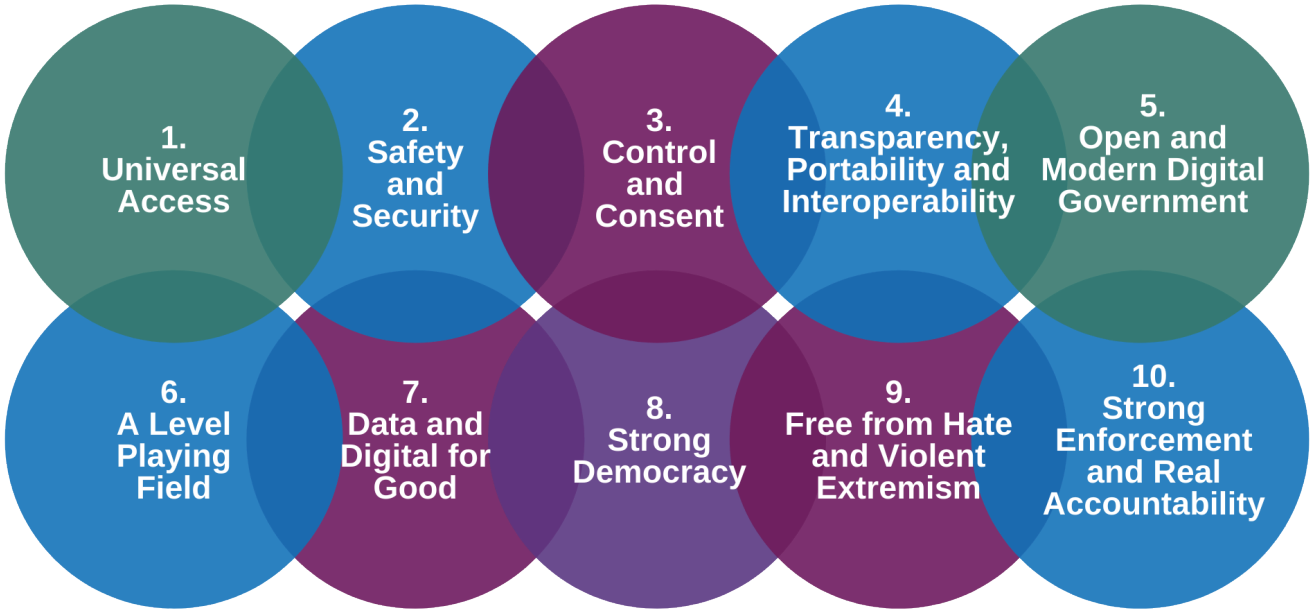
The future of digital privacy as Couvukian sees it, is one where data becomes more decentralized and moves away from the big data model. She provides the example of a Toronto waterfront development proposal where the designers intend to de-identify the data as it is collected. She argues that the technology is already there for this trend to be realized, and it presents multiple wins for all of the stakeholders.

With respect to education, Couvukian (2019) advises that schools should help students, especially young students, understand what information can be shared to collaborate and what information should not be shared.

Some Final Thoughts on the Privacy Paradox

A report that was designed to restore confidence in Canada's privacy regime (Office of the Privacy Commissioner of Canada, 2017) reminds Canadians that we need to find ways to protect privacy online in order to allow the economy to grow and to allow Canadians to benefit from innovation. This national report provides risk abatement solutions through compliance with policies and educating users of technology. The report recommends that students should learn about privacy early and learn how to anonymize their personal information. When considered alongside the recommendations of the International Working Group (2016) and the Privacy by Design directions (Couvukain, 2011), there is the beginning of a roadmap for curriculum policies aimed at educating educational institutions.

In 2011, Jennifer Stoddard, then the Privacy Commissioner for Canada, recommended that corporations should collect only the minimum amount of personal information required, and they should provide clear *unambiguous* information about how the personal information would be used. It was also advised that consumers should be provided with easy-to-manage privacy controls and the means to delete their accounts. Despite these recommendations, the privacy paradox persists although new directions for building trust in Canadian online commerce have led to the creation of this placemat of forward directions (Innovation, Science and Economic Development Canada, 2018).



Note. The 10 principles of Canada's digital charter [PDF], by Innovation, Science and Economic Development Canada, 2019.

Canada's Digital Charter outlines that modernized consent should ensure that there is plain language so that people can make meaningful choices about consent to share information. Canadians should also be allowed to withdraw consent and request that individuals dispose of their personal information. Businesses would need to be transparent about how they make recommendations or referrals to individuals and businesses would have to explain how the information was obtained. There should also be clearer guidelines with respect to the protection of individual information.

In the US, new legislation requires the US Department of Homeland Security to conduct a study on K-12 cybersecurity risks (Bradley, 2021). This legislation reportedly is a starting point for establishing national K-12 cybersecurity standards.

The answers to the privacy paradox likely reside in a combination of considerations that include:

- limits on corporations similar to European approaches;
- an appreciation of the trust that can be built for users through privacy by design;
- newer technologies to de-identify data on capture;
- more education for the end-users, including students, parents and teachers;
- an appreciation of the complexity of the privacy paradox; and
- global recognition that privacy is a human right.

For the present, schools and parents need to help students understand that their online presence is permanent. Globally, citizens need to learn that their privacy has value and that their actions can put their own privacy and that of others at risk.

References

Abrams, L. (2020, August 9). *ProctorU confirms data breach after database leaked online*. BleepingComputer. https://www.bleepingcomputer.com/news/security/proctoru-confirms-data-breach-after-database-leaked-online/

Ahlfeld, K. (2017) Device-driven research: The impact of Chromebooks in American schools. *International Information & Library Review, 49*(4), 285-289 https://doi.org/10.1080/10572317.2017.1383756

Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy, 8*(1), 21-27. https://doi.org/10.1109/MSP.2010.38

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28. https://doi.org/10.2307/25148715

Balanskat, A., Blamire, R., & Kefala, S. (2006, December 11). *The ICT impact report: A review of studies of ICT impact on schools in Europe*. European Schoolnet. http://colccti.colfinder.org/sites/default/files/ict_impact_report_0.pdf

Bradley, B. (2021, October 8). *New law requires Federal Government to identify K-12 cyber risks, solutions*. EdWeek Market Brief. https://marketbrief.edweek.org/marketplace-k-12/new-law-requires-federal-government-identify-k-12-cyber-risks-solutions/

Brend, Y. (2016, August 9). *Vancouver police admit using StingRay cellphone surveillance, BCCLA says*. CBC News. https://www.cbc.ca/news/canada/british-columbia/vancouver-police-stingray-use-cellphone-tracking-civil-liberties-1.3713042

Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles*. Privacy by Design. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Cavoukain, A. (2019, June 27). *Dr. Ann Cavoukian: Privacy by design, security by design*. [Video]. Youtube. https://www.youtube.com/watch?v=xqreZlGL8Dk

CDC. (2020, March 13). *Virus* [Photograph]. Unsplash. https://unsplash.com/photos/k0KRNtqcjfw

Coppola, D. (2022, January 11). *E-commerce in Canada – statistics & facts*. Statista. https://www.statista.com/topics/2728/e-commerce-in-canada/

Germain, (2020, December 10). *Poor security at online proctoring companies may have put student data at risk*. Consumer Reports. https://www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk-a8711230545/

Greaves, T. W., Hayes, J., Wilson, L., Gielniak, M., & Peterson, E. L. (2012). *Revolutionizing education through technology: The project RED roadmap for transformation*. International Society for Technology in Education.

Innovation, Science and Economic Development Canada. (2018). *Canada's Digital Charter: Trust in a digital world* [Graphic]. https://www.ic.gc.ca/eic/site/062.nsf/vwapj/1020_04_19-Website_Placemat_v09.pdf/$file/1020_04_19-Website_Placemat_v09.pdf

International Working Group on Digital Education (IWG). (2016, October). *Personal data protection competency framework for school students*. International Conference of Privacy and Data Protection Commissioners. http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf

Kienle, L. (2020, November 30). *Cable connection* [Photograph]. Unsplash. https://unsplash.com/photos/j48IJb5oB4k

Leatham, H. (2017). *Digital privacy in the classroom: An analysis of the intent and realization of Ontario policy in context* [Master's dissertation, Ontario Tech University]. Mirage. http://hdl.handle.net/10155/816

Leatham, H., & Robertson, L. (2017). Student digital privacy in classrooms: Teachers in the cross-currents of technology imperatives. *International Journal for Digital Society (IJDS), 8*(3). https://doi.org/10.20533/ijds.2040.2570.2017.0155

Massara, F., Raggiotto, F., & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology & Marketing, 38*(10), 1814-1827. https://doi.org/10.1002/mar.21524

Miske, I. (2017, February 13). *Home shopping* [Photograph]. Unsplash. https://unsplash.com/photos/Px3iBXV-4TU

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society, 4*(3), Article 2056305118784770. https://doi.org/10.1177%2F2056305118784770

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Office of the Privacy Commissioner of Canada (2022, January 24). *Data Privacy Week a good time to think about protecting children's privacy online*. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220124/

Office of the Privacy Commissioner of Canada (OPC) (2017). *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. Real fears, real solutions: A plan for restoring confidence in Canada's privacy regime*. https://www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf

Pierce, G. L., & Cleary, P. F. (2014). The K-12 educational technology value chain: Apps for kids, tools for teachers and levers for reform. *Education and Information Technologies, 21*, 863-880. https://doi.org/10.1007/s10639-014-9357-1

Powell, A. (2020). *An awakening over data privacy*. The Harvard Gazette. https://news.harvard.edu/gazette/story/2020/02/surveillance-capitalism-author-sees-data-privacy-awakening/

Prostock-Studio. (2020, July 24). *Digital thoughts* [Photograph]. Canva. https://www.canva.com/media/MAEC-U8QkYA

Robertson, L., Muirhead, B. & Leatham, H. (2018). Protecting students online: International perspectives and policies on the protection of students' digital privacy in the networked classroom setting. In, *12th International Technology, Education and Development (INTED) conference. Valencia, Spain, March 5-7, 2018* (pp. 3669-3678). https://doi.org/10.21125/inted.2018.0705

Robertson L., Muirhead B. (2019). Unpacking the Privacy Paradox for Education. In A. Visvizi & M. D. Lytras (Eds), *RIIFORUM: The international research & innovation forum: Research & innovation forum 2019, technology, innovation, education, and their social impact*. Springer. https://doi.org/10.1007/978-3-030-30809-4_3

Solove, D. J. (2020). *The myth of the privacy paradox*. George Washington Law Faculty Publications & Other Works. https://scholarship.law.gwu.edu/faculty_publications/1482/

Statista Research Department. (2022, Feb. 14). *Facebook: number of monthly active users worldwide 2008-2021*. Statista. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Steeves, V. (2014). *Young Canadians in a wired world, Phase III: Life online*. MediaSmarts. http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf

Stoddart, J. (2011). Privacy in the era of social networking: Legal obligations of social media sites. *Saskatchewan Law Review, 74*, 263-274. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sasklr74&div=20&id=&page=

UNICEF. (December 1, 2020). *Two thirds of the world's school-age children have no internet access at home, new UNICEF-ITU report says*. UNICEF United Kingdom. https://www.unicef.org.uk/press-releases/two-thirds-of-the-worlds-school-age-children-have-no-internet-access-at-home-new-unicef-itu-report-says/

US Department of Education (n.d.) *Use of technology in teaching and learning.* Office of Elementary & Secondary Education. https://oese.ed.gov/archived/oii/use-of-technology-in-teaching-and-learning/

Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. *Fundamental Research, 1*(5), 543-551. https://doi.org/10.1016/j.fmre.2021.08.009

Wikipedia contributors. (2022, February 8). *Paradox*. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Paradox&oldid=1070583071

7.

DIGITAL PRIVACY COMMUNICATION TOOLS AND TECHNOLOGIES

James Robertson

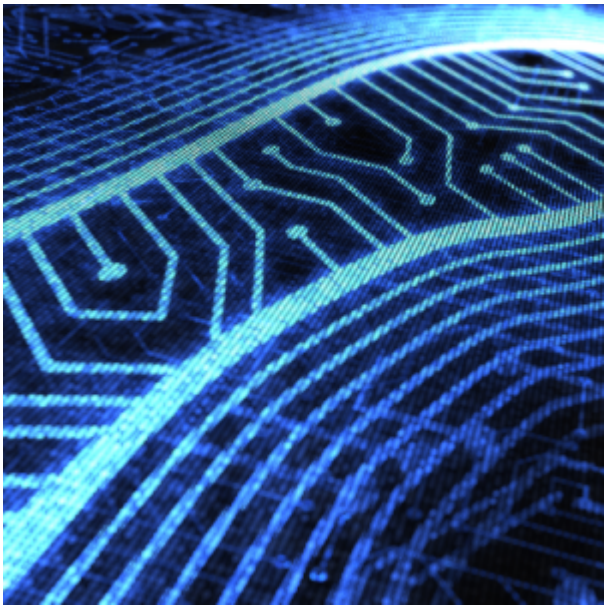
This chapter will assist students with the following tasks:

1. Define digital footprint and its elements.
2. Identify ways to prove identity online.
3. Learn how online shopping, banking, and finances impact digital privacy.
4. Explain the role of web browsers, search engines, and browser add-ons in managing your digital footprint.
5. Identify the ways that Virtual Private Networks, proxies, and data encryption can work to limit the collection of private information.

Topics in this chapter:

1. Managing your digital footprint.
2. The importance of *identity and access management* (IAM) online.
3. Secure online shopping and banking.
4. Challenges and tools for secure web browsing.
5. The role of email in digital privacy.
6. Secure messaging, calling, video applications and tools.

Managing your digital footprint



Note. Digital footprint, by Alengo, 2011.

The term *digital footprint* refers to the trail/traces of digital information (or data) that you create – and others collect – by your online activity (Muhammad et al., 2017). This includes web browsing (the sites you visit, the videos you watch, anything you click on), your Google searches, any text you type, the forums you contribute to, anything you upload or download, the IP address of your computer/device, your location, and more. Your digital footprint is permanent, but it can be managed. According to Carrothers (2018), the average American had 200-300 online accounts in 2020, and that number will soar to 300 by 2022. This number of passwords is already virtually impossible to memorize, and it is growing. Consider instead the efficiency of a password manager.

Without checking your computer, take a few moments to identify your online services, apps, forums or websites for which you have a login (Username and Password). Next, write down the usernames, email addresses or cell phone numbers you have used when you signed up for a web-based tool, service or account.

- Visit https://haveibeenpwned.com/ and check your username(s). Similar tools include https://www.namechk.com/ and https://knowem.com/.
- Visit https://www.avast.com/hackcheck/ and check your email addresses.
- At the https://haveibeenpwned.com for example, you can see where there may have been a breach associated with your email or phone number. You will also be able to see the billions of persons whose information has been breached.

Here are some tools to manage your digital footprint:

1. Use the Google search for your full name, username(s) and email address(es).

- Try variations of your name (spelling, short forms).
- Use search qualifiers (Boolean Operators) such as intext: John Doe (where John Doe is your first and last name) in the Google search field.
- Modify the above search to add things like your organization or place of employment, city, places where

you volunteer, committees to which you are a member, etc.
- Try searching your name in Google Images.
- Try searching your cell/home/work phone number(s).

2. You can complete the searches in other web search engines as well (e.g., DuckDuckGo, Bing, Yahoo, Qwant, or Yandex).

3. Check out online identity information aggregation tools such as PeekYou.com and Spokeo.com.

When you take the time to access these tools, you will learn much more about the extent of your personal digital footprint. Take a critical stance toward the personal information about you that is *out there* and calculate your level of comfort with the associated risks.

Identity and Access Management Online

There are *identity and access management* (IAM) tools that can help you identify yourself online, protect your identity and manage your digital footprint. Here are some of the key terms:

Attribute	Explanation
Identity	• Who you are (e.g., username)
Authentication	• How you prove who you are (e.g., password/PIN)
Authorization	• What you can do
Access	• What you are allowed to see • Where you're permitted to go
Accounting	• What you did while online
Verification	• How a system makes sure the information you share is accurate (e.g., sending an email/text to make sure you have access to them)
Validation	• Taking ownership of your identity through personally identifiable information

Authentication: Authentication is how you prove your identity. You have some authentication options. Authentication is usually accomplished through a combination of three elements:

- Something you **know** (e.g., password or personal question).
- Something you **are** (e.g., biometrics).
- Something you **have** (e.g., smartphone, swipe/prox/chip card, dongle or other hardware keys).

Of these three, something you know (e.g., username and password) is the most common method. Personal knowledge-based questions are often used as an alternate method of verification. Biometric identification is considered the most secure. Some authentication apps (e.g., Duo, Google Authenticator) are increasing in popularity, as are password keepers/managers.

Passwords are a popular means of ID management but there are definitely risks if users reuse their passwords

across applications. There are multiple changes happening in the world of password management. Organizations are now routinely requiring password updates and changes. Passwords are giving way to passphrases as passphrases are more difficult to guess. Other types of authentication methods are emerging such as one-time passcodes over SMS or email. There is also an increase in *single-sign-on* (SSO) solutions for employees. As a result, Password Managers (or *keepers*) are increasing in popularity (e.g., 1password, Lastpass, Dashlane, Bitwarden, Google Password Manager).

Consider the use of alias users, temporary accounts, designated SIM card/smartphone. Some tools to consider for maintaining identity privacy include the use of:

- **Alias users**. You can have more than one email address to your email account. Let's say that your work name is elizabeth.bold@mail.com but your friends know you as Liz or Betty. You can create alias user names to the same email account.
- **Temporary/disposable email accounts**. You may elect to create an account through a *disposable* account which often limits the collection and aggregation of your personal information. Consider the use of disposable email addresses such as Mailinator or Maildrop for verification emails.
- **Designated SIM card/smartphone**. This is an alternate SIM card—usually with an inexpensive, data-only plan, that allows you to provide a cellphone number at the time of account creation and maintenance (ex. password reset).
- **Calculated security questions**. By not giving truthful answers when setting up *security questions* you limit the potential for scaffolded attacks if a data breach occurs.
- **Avoid recycling usernames and passwords**. Make usernames that are app-specific (e.g., Johndoe-Facebook, Janedoe-Twitter).
- **For more ideas**, check out the *New York Times* article How to Protect Your Digital Privacy (Klosowski, 2019).

Secure Online Shopping and Banking

Note. Luminous laptop, by P. Katzenberger, 2019.

Today's digital banking affordances make it easier to manage your finances, pay bills and send money online. Lake and Foreman (2021) report that 57% of consumers say that they prefer online banking to in-branch banking, but this raises privacy issues. Reflect on what and how you purchase online and how the pandemic has affected your online purchasing. Lake and Foreman report that consumers are not always proactive about protecting their personal and financial information (2021). A recent study found that only 42% of Americans using online banking have separate passwords for separate accounts, and only 23% of Americans reported that they use a password manager (Lake & Foreman, 2021).

Here are some suggested tools for securing online payments and banking:

- Use only secured sites (indicated by https:// at the beginning of the URL);
- Never give your banking PIN/password over the telephone or by email; No legitimate bank will ever ask for it!
- Monitor your accounts weekly for fraudulent activity;
- Set up limits on your credit card purchases with your bank;
- Ask for *2-factor authentication* (2FA) for any purchases/transactions. (e.g., SMS (text) confirmation);
- Do not conduct online banking or purchases over public/open wireless networks;
- Confirm suspicious emails with your bank (or the seller) prior to clicking anything;
- Use secure passwords for e-transfers; and
- Consider using a credible third-party to mediate online purchases (to avoid sharing your banking information with the seller).

Web Browsing: Best Practices

Web browsing (aka *web searching* or *Googling*) is the original and most common internet function (after communication), yet it still poses significant privacy risks. Web Browsers are computer applications that provide the user with the interface through which they can access the internet's (world wide web) websites, data, and documents. Web browsers applications vary with respect to functions, features, and security/privacy

tools. The most common web browsers are Internet Explorer/Edge, Google Chrome, Mozilla Firefox, Opera, and Apple's Safari. Your activity online (e.g., web browsing) HAS VALUE and can be monetized by website providers. The most common tracking methods include browser cookies, IP addresses, and usernames.

Cookies are made up of data that your browser creates, stores, and exchanges with various websites you visit in order to personalize and expedite your web browsing. Provider cookies are not all bad, and can be very useful, but avoid *third-party cookies*—these are the ones that collect your data for the purpose of sale/profit (usually in the form of advertising). Other types of cookies include tracking cookies (when was the last time you visited the site, how long you were there, what you clicked on, etc). When you connect to the internet, your device gives information to the server on the website that you visit. This information is called a device fingerprint, a machine fingerprint or a browser fingerprint. Hauk (2022) explains that, "Browser fingerprinting is a powerful method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution and various other active settings" (pp. 6). Some browsers such as Chrome and Safari allow the user to restrict certain types of cookies.

Here are some tools to ls to protect privacy while browsing the web:

- Check to see if your browser has a *privacy mode* such as *Incognito Mode*. Use this mode especially if using a shared computer.
- There are web browsers that were created with privacy as the primary function; examples include DuckDuckGo, Brave, TOR browser, Waterfox, Epic.
- Clear your browser cookies regularly.
- Consider using a VPN service before browsing.
- Exit the browser when not in use. Most browsers can be set to clear cache/cookies upon exiting the application.

There are other privacy-enhancing tools such as: using VPNs, Proxy addresses and data encryption.

VPN: A Virtual Private Network

A VPN is like a tunnel that only has two openings: one sender and one receiver. Data between these two parties travel in/through the tunnel but can't leave the tunnel except via one of the two openings. While in the tunnel, data cannot be added, modified, or removed by any third parties. This secure tunnel between sender and receiver is possible through something called *encryption*. Encryption is the process of masking (or changing) data so that only the intended recipient can read it. To anyone else, the data is unreadable. VPNs disguise your data so that it cannot be intercepted while in transit across the internet. VPNs also change the IP address your device broadcasts, which helps protect your location as well. It is similar to a proxy server. Nadel (2020) states that the beauty of the VPN is that it can turn your computer into an *anonymous machine.*

Proxy Server

Unlike VPN's which encrypt/secure all data exchanged during a session, Proxy Servers are used only to mask/change the IP address your device broadcasts with a different IP address generated by the proxy server. Since privacy and location data can be inferred via your IP address, there is value in protecting this piece of private information while browsing. Proxy servers do not encrypt your data. Some *free* proxy servers will log your information and sell that information to others for profit. A proxy server is not required if you are using a VPN service

Data Encryption and Privacy

Encryption is a concept that has been around for centuries – not a new concept. It involves protecting an important message from being read/modified even if the message is intercepted while in transit from sender to receiver. The study of encryption is called cryptography. In computing terms, encryption is usually done via complex mathematical algorithms and uses a set of protocols – the rules used to encrypt (and later decrypt) a message. Unencrypted data is called *plaintext* data and can be read by anyone. Encrypted data is referred to as ciphertext. You can encrypt data in transit using a VPN, but you can also encrypt data at rest on your device. You might choose to encrypt an individual file, folder, or entire drive. Encrypted files are usually protected by a password.

Note. Glowing lock icon, by A. Oleshko, 2018.

The Role of Email in Digital Privacy

Tools To Manage Privacy Through Email

Email is the primary tool for business communication. *Electronic mail*—email—was created at the same time as the first computers. Email is a form of asynchronous messaging – meaning a server stores the email until you log into that server to retrieve it. Conversely, *instant messaging* (IM) is a form of synchronous messaging. Despite its age, email is a communications/messaging platform that continues to grow, with a projection of over 330 billion emails sent per day by 2022 (Radicati Group, 2018). An email account/address is integral to

the overall internet experience, with most services requiring email-based verification for new users. Email is also the most common attack vector for cyber attacks, with experts estimating that "an individual's email account is more likely to be broken into than their house" (Waschke, 2017, p.3).

By default, email sends in plain text, making it one of the least secure forms of electronic communication. Email allows malicious actors to instantly reach thousands of users around the world with a single click. Private information can be inadvertently shared by email users through the following means: social engineering emails, phishing or spear-phishing emails, *personal health information* (PHI) requests, and banking or financial fraud. For some reminders about PII from the U.S. Department of Education's (2016) perspective, watch Personal cybersecurity: How to avoid and recover from cybercrime [2:53].

Email Privacy Tools and Tips

- Enable 2FA to access your email.
- Move sensitive emails off your email server (your inbox) and into an encrypted file on your device or cloud.
- For sensitive emails, use an email service that was designed with privacy in mind.
- Never open attachments until you confirm with the sender.
- Create multiple email accounts that are used for different purposes (work, personal, financial, social, news/subscriptions, etc) and sort/forward the useful email to your private account (the one that you never provide to anyone).
- Use a VPN when accessing your web-based email account(s).
- Be suspicious of every message! Carefully check the sender's address. Hover over any links (to see the URL's without having to click).
- Never include PII in the body of an email – regardless of the recipient.

Some email services are designed with privacy at the core. ProtonMail, Hushmail and Tutanota are examples of email providers that provide encryption and other privacy-enabling tools (such as aliases and expiration dates). Consider using disposable or temporary email services for verification purposes. Examples include:

- https://www.guerrillamail.com/
- https://10minutemail.com/
- https://www.throwawaymail.com/

Note. Encrypted spreadsheet, by Matejmo, 2018.

Secure Messaging, Calling, and Tools

Traditional text messaging—also called *Short Message Service* (SMS)—was the original form of text-based messaging on cell phones. As cell phones evolved into smartphones—which included built-in cameras and applications (or *apps*), there came a concurrent desire to send photo/video content via text messaging. *Multimedia Message Service* (MMS) was created to meet this need. Neither SMS or MMS messages are encrypted, which means messages can be intercepted and read as plain text by others. The desire for increased privacy in text messaging gave rise to encrypted messaging apps designed to protect communications by ensuring only the intended sender and receiver(s) have access.

Encryption is the most popular method of securing data such as instant messages while in transit across a network. Secure messaging apps will encrypt message data in transit and at rest. This is called *end-to-end* (E2E) encryption. Popular secure messaging products include Signal, Wickr, Wire, Telegram, Threema, Viber, and Apple's iMessage. Other applications like Instagram, Twitter, Facebook Messenger, WhatsApp, and Snapchat are encrypted in transit but not at rest—and therefore not E2E. For example, the Meta/Facebook family of messaging apps (Instagram, FB Messenger, and WhatsApp) are encrypted from other parties but not from Meta/Facebook, who can view, save, and analyze messages sent on these apps.

Secure Messaging for Video and Phone Calls

Due to the pandemic and the resulting trend to work and learn from home, more people are using digital tools to communicate in both audio and video formats. Popular video calling tools include Zoom, WebEx, Skype, Google Meet (or Duo), GoToMeeting, Bluejeans, Microsoft Teams, and Apple's FaceTime. For telephone calls (audio only) encrypted communications are possible through a technology called *Voice Over Internet Protocol* (VOIP). VOIP calls convert our spoken words (audio) into digital format and encrypt those data before transmitting them to the other party. The receiver decrypts the message and converts it back to audio format. This enables secure voice calling.

Lee and Grauer (2020) explain that while Zoom supports E2E encryption it does so at the cost of other key functions and features, as well as requiring Zoom users to configure security functions. Zoom's (2021) white paper on security provides a list of security functions such as logins, but Lee and Grauer report that it is not E2E encryption but rather the type of encryption called *Transport Layer Security* (TLS). TLS is used to secure data transmitted to and from HTTPS websites. On the other hand, FaceTime conversations are reported to be private because FaceTime uses E2E encryption (TechBoomers, 2017).

Privacy in Social Media

Social media sites and platforms are highly interactive online spaces that support interpersonal communication, the creation and maintenance of social connections, and the sharing of digital content and resources that are primarily user-generated. They support the creation of communities (also called social networks)—both personal and professional—that support learning, idea-sharing, conversations, opinions, and interests. Users create member accounts, create profiles, and connect with other information sources, people, and organizations. First iterations of social media platforms emerged in the late 1990s and early 2000s. Popular platforms include Twitter, Instagram, Facebook, TikTok, YouTube, LinkedIn, Snapchat, Pinterest, Reddit and Discord.

User-generated digital content is the lifeblood of social media sites. Users share content they create. Their likeness, home address, names of family members, personal identity information, place of work, political affiliation, relationships, race, gender identity, medical conditions, physical location, financial status and a myriad of other PII is openly shared (and permanently recorded). Further, in order to personalize the user experience (UX), social media sites request personal information from the user in order to suggest connections, contacts, news sources, and other digital content of interest. This information can be sold for significant profit to advertisers and other interested parties.

Facebook's average annual revenue is $55 billion. The company's net worth is nearly a trillion dollars. Many of the privacy concerns in social media stem from users who voluntarily post private information on social networks. Madden (2012) in an early study of privacy management on social media sites, found that the oldest users and the newest users were the most careful about their privacy settings on social media. It may be that some of the data privacy-protective models will emerge from models employed by the American military (e.g., Davison et al., 2021).

Tools and Strategies for Privacy when using Social Media

- Check the privacy settings associated with your social media account. Every social media site has these settings.

- Use an email address/account dedicated to that platform (e.g., Tdorian33.facebook, tdorian33@gmail.com, tdorian33.twitter, etc.).
- Assume that your posts, comments, content, videos, photos, and audio can be accessed by people other than the intended recipient(s).
- Do not post or share PII such as birthday, cell number, banking info, health info, usernames and passwords, vacation plans, relationship info, etc.
- Remove all geotagging and Exif data from any images you post (e.g., *selfies*).
- Confirm connection requests PRIOR to accepting them. Confirmation by phone or email works best.
- Avoid surveys and quizzes that ask you to provide partial information (e.g., month of birth, first initial, year of birth, gender identity, age ranges).
- Use multi-factor authentication to access your social media apps.
- Avoid login options such as "log in using Google" or other accounts.
- Avoid *tagging* people in the photos you post/share with others.
- Many social media users seek to have many followers, likes, and upvotes. Chasing these metrics may result in posting something you might regret.
- Consider digital permanence; once it's posted, you lose control over it.
- What you post may be shared with your professional circles, so post carefully.
- Close unused accounts and delete data beforehand.

For a fuller explanation of these tools, see the Office of the Privacy Commissioner of Canada's (2019) post staying safe on social media (2019).

This chapter focused on the various digital tools and technologies used in the way we communicate digitally, and the role those technologies play in the protection and preservation of our digital privacy. The definition of digital privacy in this e-book is the *expectation* of privacy unless *informed* consent has been given. This definition includes the understanding that digital persons can exercise some *discretion* with respect to how and where they share their digital information. The description of the tools and technologies in this chapter was designed for that purpose.

References

Alengo. (2011, September 07). *An abstract image of a digital footprint* [Photograph]. Canva. https://www.canva.com/media/MAEJHU4HMk8

Caruthers, M. (2018, May 11). *World password day: How to improve your passwords.* Dashlane Blog. https://blog.dashlane.com/world-password-day/

Davison, C. B., Lazaros, E. J., Zhao, J. J., Truell, A. D., & Bowles, B. (2021). Data privacy in the age of big data analytics. *Issues in Information Systems, 22*(2), 177-186. https://doi.org/10.48009/2_iis_2021_185-195

Hauk, C. (2022, February 17). *Browser fingerprinting: What is it and what should you do about it?*. PixelPrivacy. https://pixelprivacy.com/resources/browser-fingerprinting/

Katzenberger, P. (2019, January 21). *Luminous laptop* [Photograph]. Unsplash. https://unsplash.com/photos/iIJrUoeRoCQ

Klosowski, T. (2019, May 03). *How to protect your digital privacy*. New York Times Privacy Project. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Lake, R. & Foreman, D. (2021, April 05). *Increase in digital banking raises consumer data privacy concerns: how to protect yourself*. Forbes Advisor. https://www.forbes.com/advisor/banking/digital-banking-consumer-data-privacy-concerns/

Lee, M. & Grauer, Y. (2020, March). *Zoom meetings aren't end-to-end encrypted, despite misleading marketing*. The Intercept. https://theintercept.com/2020/03/31/zoom-meeting-encryption/

Madden, M. (2012, February 24). *Privacy management on social media sites*. Pew Research Center. https://www.pewresearch.org/internet/2012/02/24/main-findings-12/

Matejmo. (2018, February 02). *Encrypted spreadsheet* [Photograph]. Canva. https://www.canva.com/media/MAEE1UdvCws

Muhammad, S. S., Dey, B. L., & Weerakkody, V. (2018). Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: A systematic review of literature. *Information Systems Frontiers, 20*(3), 559-576. https://doi.org/10.1007/s10796-017-9802-y

Nadel, B. (2020, April 16). *How to use a VPN to tighten security for remote teaching*. Tech & Learning. https://www.techlearning.com/how-to/how-to-use-a-vpn-to-tighten-security-for-remote-teaching

Office of the Privacy Commissioner of Canada. (2019, August). *Staying safe on social media*. https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/social-media/02_05_d_74_sn/

Oleshko, A. (2018, May 18). *Glowing lock icon* [Photograph]. Canva. https://www.canva.com/media/MADesctbO30

Radicati Group (2018). *Email statistics report, 2018-2022*. The Radicati Group, Inc. https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf

Techboomers. (2017, April 21). *Is Facetime safe, private and secure?*. https://techboomers.com/t/facetime-safety-security-privacy

U.S. Department of Education. (2016, October 12). *Email and student privacy* [Video]. YouTube. https://youtu.be/hm82nRxi0yg

Waschke, M. (2017). *Personal cybersecurity: How to avoid and recover from cybercrime*. Apress: Springer. https://doi.org/10.1007/978-1-4842-2430-4

Zoom. (2021, August). *Security guide: White paper*. https://explore.zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

8.

TODAY'S DEVICES AND TOMORROW'S TECHNOLOGIES

James Robertson

This chapter will assist readers with the following tasks:

1. Identify the digital devices in your home or on your person that collect personally identifiable information.
2. Describe the steps you can take to manage the information that these devices share across their personal, professional, and public networks.
3. Critically examine the kind of information collected and stored on wearable devices, and recognize the value that these data have to others.
4. Discuss the benefits of smart home devices such as digital assistants and smart speakers, along with the risks presented by the continued use of these devices.
5. Recognize the threats and risks inherent in home networks—both wired and wireless—with respect to the potential for digital privacy breaches.

This chapter examines the impact of your digital, connected devices on the privacy of your personal information. In particular, this chapter identifies common digitally-connected devices found in most homes and the amount of data these devices have access to collect and share. Devices such as your home computer, laptop, tablet, and smartphone are discussed, along with less obvious devices such as webcams (both internal and external), external storage devices, smart appliances, and smart home management tools. Among those tools are connected video doorbells, home security and video surveillance cameras, thermostats, lighting, gaming consoles, and smart speakers (digital assistants).

In addition to the devices in your home, this chapter also explores the devices that you wear on your body or carry with you. Such devices include activity trackers, smartwatches, digital wallets, implants, smart glasses,

GPS wayfinders, and medical devices. This chapter will also venture into a discussion on the privacy risks involved in home networks—namely wireless routers and access points, physical or virtual firewalls, and Bluetooth-connected devices.

Your Devices and Privacy—An introduction

Note. Digital devices, by Firmbee, 2015.

The above introduction uses the term *digital device*. Definitions of devices vary, which warrants a section for the definition of key terms used in this chapter. It is suggested that readers create a chart or similar method of documenting new terms (and their definitions) and update this chart continuously while engaging with the chapters in this text. Alternatively, you can go to any online flashcard creator. I like brainscape.com for online flashcards and Anki for offline (but shareable) digital flashcards. Build your own custom flashcards and then share them with your colleagues, classmates, friends, and peers who are also interested in digital privacy.

A digital device is defined as any electronic device that uses digital technology to function. It is a device that can send, receive, store, and process data (information in binary form). The opposite of digital devices is analog devices—or devices that do not have/use embedded computers, CPU, microprocessors, microcontrollers, or embedded circuits. Analog devices are those that use manual switches, dials, and/or electrical power.

Many, but not all, digital devices have communication chips included that allow the device to connect either directly to the internet or to the main controller (that is on a network). There are many digital devices that cannot connect to anything. Take, for example, your old digital watch, alarm clock, or television as examples of devices that may not be connected. Your old car is another example; however, as society increasingly expects and demands a hyper-personalized digital experience, many of these traditional devices are now being manufactured with the ability to connect to other devices in the home as well as to the internet (or they are retrofitted).

Reflection Activity

Consider your own devices. How many are *smart* (connected) and how many are not? If you have smart devices in your home, for what reason did you purchase them?

Section 1: Mobile Devices and Privacy

Mobile devices, such as smartphones, laptops, tablets, portable hard drives and USB keys, can hold huge amounts of sensitive personal information. It's important to take measures to protect the data on these devices from loss; theft; and threats, such as viruses and spyware (Office of the Privacy Commission of Canada, 2020).

Mobile devices collect incredible amounts of private information, including messages, emails, phone calls, location data, health information, banking/financial accounts, images and videos of a private/personal nature (e.g., pictures of your children or of your driver's license), lists of tasks, contacts (friends, coworkers, family), your meetings, where and how you shop, which websites you visit, usernames and passwords, biometric information, and more. The list seems endless—and in some sense, it is, because you are constantly creating new data via your smartphone.

Reflection Activity

Try to make a list of the information you would categorize as *private*. Does your device ***need*** this information to function properly?

Managing Privacy Information on a Smartphone

"It's hard to overstate how much of our personal lives we can potentially reveal to our smartphones."

(Privacy Rights Clearinghouse, 2017)

Many computing devices—including smartphones—have a setting for the user to manage permissions. This is a function added to smartphones and other smart devices to allow the user some control over what data the device can collect, save, store, and share. On a smartphone, for example, permissions can be as granular as deciding which of your mobile apps can access your location, your contacts, your files (pictures, videos, emails, text messages), your cameras, and your microphone to record audio.

Personal Reflection

Locate the *permissions setting* on your phone. Look through which apps have what permissions. Any surprises? Do the apps on your phone need this access in order to function?

Note. App-based games will often require the user to grant permissions to the app before the game can be played. In fact, some apps harvest our data even when we deny them access to personal information and the situation seems to only be getting worse with each passing year (Mikalauskas, 2021, para. 2)

Similar settings can be found on your tablet, laptop, computer, fitness/activity tracker, and so on. Familiarize yourself with these settings. Many applications collect data about you (that they do not need) in order to sell that information to third-party marketing firms. The revenue from the sale of this data allows the app creator/provider to make a profit while providing the app at *no cost* to the consumer. Recent research by pcloud.com identified a number of mobile apps that tracked and shared/sold your data; Facebook, Instagram, and food delivery apps were among the top culprits (Dimitrov, 2021). This same study found that "52% of mobile apps share your data with third parties" (para.7).

Another method app vendors will employ to generate revenue is to offer free versions of their app, but they

restrict functions and features to the paid version. There is some merit to paying for your privacy. In a recent article, Thorin Klosowski (2021) found that paid versions of apps "don't have ads and so don't benefit directly from collecting data about you" (para. 26).

Section 2: Computers and Operating Systems

In addition to all the newer digital devices, tools, and services, home desktop computers and laptops continue to increase in popularity (Alsop, 2022). Given the recent trend of workers completing their work from home, the demand for desktop computers and laptops has increased (Foran, 2021). Multiple studies report personal computers to be second only to smartphones in terms of personal computing device sales. In fact, according to PEW Research (2015), 80% of homes in the US had a personal computer. According to the United States Census Bureau data from 2018, that number rose to 92% of households that had at least one type of computer and 85% of homes had a broadband internet subscription.

In addition to the work-from-home trend brought about by the pandemic, the popularity of desktops and laptops can be attributed to increased use of personal computers for online gaming, streaming services (like Netflix), and the general belief that hard-wired internet is faster, safer, and more reliable than wireless communications (Paus, 2018). Computers run operating systems to facilitate the user interface. Windows 10 is the world's most widely adopted operating system, running on three out of every four desktop computers and is installed on over 1.4 billion devices (Mehdi, 2020).

However, despite widespread—and increasing—adoption, personal computers and laptops are not without risks and challenges. For example, a) these devices are not as portable as tablets or smartphones; b) they must be connected by wired or wireless devices and cannot connect to mobile networks; c) they are usually large and often need dedicated room/space; and d) they are often shared among all users in the house, require constant/uninterrupted power, and can be expensive. Personal computers often require peripheral devices for users to efficiently operate, including a mouse, monitor, keyboard, webcam, speakers or headphones, external hard drives, and USB keys. Very few personal computers support touch screen interfaces, and therefore, require a higher level of digital literacy to operate. Lastly, and this is not unique to personal computers and laptops, they pose security risks to children who browse, watch, and chat with strangers online without supervision.

Protecting your Privacy on Personal Computers

There are alternatives to Windows operating systems, such as Linux distributions like Ubuntu, Linux Mint, and Zorin OS. Another option is to use virtual machine (VM) software, which allows a computer user to separate, isolate, and segregate (a process called *sandboxing*) their primary operating system from other, riskier tasks such as web browsing, downloading files, sharing files, and reading emails.

In order to protect your privacy in a personal/home computer, consider these suggestions:

1. Use physical tools to cover devices like webcams and microphones.
2. Make sure you lock or log out of your computer every time you step away from it.
3. Install antivirus software (there are many options with minor differences) and/or the security measures built into the operating system (e.g., Windows Defender).
4. Update your operating system and other software regularly.
5. Use whole disk encryption on your PC and store your files on encrypted external hard drives using frequent backups (this protects against ransomware as well).
6. Turn off your home router when you are asleep or away from home.

Reflection Activity

Witkowski (2022) suggests that the global pandemic is partially to blame for the massive growth of personal computers and operating system adoption as an unprecedented number of people were thrust into working from home. In what ways have working from home impacted personal privacy? What are the positive and negative privacy implications? Consider factors such as webcams, the confidentiality of information, cyber (or information) security, remote access and authentication, and stress levels.

Section 3: Wearable Devices and Privacy

In keeping with the suggestion that you collect key terms used in this chapter, let's define another—often nebulous—technical term as we define and describe what is a wearable device. In this section, we will review wearable devices and other tools to secure your conversations, messages, and video calls.

Wearable devices (or simply *wearables* for short) go by many names, including wearables, fashion tech, fashion electronics, skin electronics, and tech togs. It is generally accepted that wearables are the devices you wear on your body—either directly on your skin or with your clothes—that store, collect, process, or share digital information. These are often worn for extended periods of time.

It is important to note that not all wearable devices are *connected* to the internet (IoT devices). Wearables include devices like fitness/activity trackers and step counters, smartwatches, MP3 players, smart glasses/eyewear, HMD/HUD, safety gear (personal alarms, fallen person), health tracking equipment (medical devices), smart jewelry, GPS locators (for children and vulnerable people), smart clothing, authentication/access control devices (to unlock a door, start a car, log into a computer), and workplace/employee trackers. According to Market Research Engine (2021), the wearables industry will exceed $95 billion globally by 2026.

Benefits of Wearable devices

Wearables have exponentially increased in popularity for a number of reasons. The primary driver to date has been healthcare and health benefits due to the highly personal and private information these devices can collect, analyze, and report. Wearables can measure fitness/activity levels, heart rate, blood pressure, positive reinforcement, movement reminders, and more.

Note. Smartwatch, by N. Shaabana, 2019.

There are also safety benefits to wearables, including location trackers, hands-free use, and personal alarms—also called panic alarms—that are either manually or automatically activated. For example, the Apple Watch now has fall detection (as shown in this Apple-watch commercial). The Apple Watch will also enter emergency mode, which causes the watch to display your medical information to first responders. Other examples of personal/panic wearables include the Ripple 24/7 personal/panic alarm and the Revolar device. Fall detection wearables specifically designed for seniors, such as Lifestation Mobile and SureSafeGo, are also increasing in popularity as the average age of Canadian citizens continues to rise (Statistics Canada, 2021b). Wearables for children are also gaining popularity (in terms of locating lost children), as are health devices that monitor blood sugar levels using *continuous glucose monitors* (CGMs).

Many wearables need to connect with a smartphone in order to maximize their functions and features. These connections usually rely on Bluetooth and then leverage the smartphone's cellular or wi-fi connectivity to operationalize the data being recorded. This communication works both ways, with many wearables now able to display incoming calls and text messages to the user without the user needing to access their phone. Wearable providers rely on this app-to-wearable connection to collect data that can be monetized and/or analyzed to personalize the user experience.

A wearable connection to the internet—via the smartphone—leads to another tangible benefit, that of the

ability to make payments using the wearable device. As we move to an increasingly cashless society (Holzhauer, 2020), wearables may be a factor in reducing the number of muggings and other financial crimes such as counterfeiting.

The last benefit to wearables—and perhaps the most obvious—is that they are portable. These devices and sensors are lightweight, inconspicuous, and connected. Many wearables double as fashion accessories, making these devices not only functional but fashionable as well. This, perhaps more than the other benefits listed above, are what Caldwell (2019) attributes to the popularity of wearable devices. In addition to being fashion accessories, wearables can now also be found in our clothing for health or activity monitoring, as evidenced by this example of GPS enabled sportswear for female athletes and body roll sensors for competitive swimmers.

Challenges with Wearable Devices

Although there are many benefits to wearables, they also come with some risks and challenges. From a privacy perspective, the foremost of these lies in the volume of personally identifiable and private data that wearables collect, track, analyze, and share. Examples include location history, health status and history, place of employment, financial information, microphones (calls/audio), cameras, search history, personal messages, contacts, and more. These devices were designed with an emphasis and priority on ease of use and functionality—not privacy or security. If compromised, the data of these devices could be sold or abused, which is what occurred in this article from HealthITSecurity.com (McKeon, 2021).

Other challenges with wearables include battery life, which can be short and reduced over time, requiring frequent charging. Wearables must also be worn or removed depending on activity, may interfere with or influence other electronic devices, can cause skin irritations, are often inaccurate (for example, step counters, heart rate, and even location), and are usually expensive—especially when the device is web-connected or Bluetooth-enabled. In fact, according to research by Gartner (2016), approximately one-third of users abandon their wearable devices due to perceived usefulness, boredom, or breakage.

Reflection Activity

As you reflect on the sections so far in this chapter, ask yourself the following questions:

- What is the horizon with respect to health/identity information, human augmentation, covert surveillance/scanning and location tracking?
- What are the *privacy-protection options* for wearable users? Are there indications that users can have either privacy or wearables, but not both?
- Consider subcutaneous implants and smart tattoos, or retail purchases via your device. Do these present different privacy risks?
- To what do you attribute the growth and popularity of wearable devices despite the privacy implications and risks to personally identifiable information?
- How might wearable devices be used in education?

As you reflect, consider the following scenario and your response to it:

Cynthia is pulled over because her smart/wearable device notified police that she was driving with a blood-alcohol level above the legal limit. The police officer states they would not have stopped the vehicle on suspicion of driver intoxication based on observations alone, and only stopped the vehicle because of the device's report.

- Is this a violation of Cynthia's privacy?
- Is this an ethical issue?
- Other than Public Safety, which other sectors/industries might use information like this?

Section 4: Smart Home Devices and Privacy

What is a smart home device? According to Qashlan et al. (2021), smart home devices are growing rapidly but pose significant privacy concerns. A smart home device can be defined as any electronic device that has data processing ability ***and*** the ability to connect to other devices, controllers, or networks (like the internet). These devices often automate tasks that were previously performed by a person and allow for a variety of user input/interface options, including physical buttons, voice commands, smartphone apps, sensor or time-based automation, or artificial intelligence.

You may see smart home devices also referred to as smart home gadgets. Examples include digital assistants, televisions, thermostats, doorbells, lights, vacuums, windows, fridges, electrical outlets, cameras, burglar alarms, exercise equipment, sound systems, toothbrushes, lawnmowers, lawn sprinklers, structural sensors, and even garage door openers. Smart home devices have risen to prominence in large part due to the homeowner's desire to be aware of, but not necessarily responsible for, the operation of the many devices in the home.

There are numerous benefits to smart home devices. A study by PEW Research Center (2017) found that "nearly one-in-five American households (18%) are *hyper-connected*—meaning they contain 10 or more of these devices" (para. 4).

Benefits of Smart Home Devices

Among the benefits of smart home devices is their capacity to save homeowners money on electricity, water, gas (heating) and other home operating costs. This is accomplished by raising awareness of utilities' use, metering utilities during peak times, and turning powered devices on and off only when needed. An example is the Nest thermostat, which, upon detection (or manual input) that you have left work, turns on the heat in your home.

Note. Digital thermostat, by D. LeFebvre, 2018.

Beyond utilities, smart home devices also save money by being more efficient. For example, they can save you time by automating some tasks such as grocery shopping. Smart fridges can order from Amazon if they detect that groceries are low; autonomous vacuums can clean on a set schedule; lawnmowers can cut the grass when they detect that the grass is too long; and alarm clocks can monitor sleep patterns and raise or lower heat and lighting to maximize the quality of sleep. The list goes on.

Smart homes can also be safer and more secure through the use of controllers (hubs and smartphones), sensors, and security devices such as video surveillance cameras to monitor people and property. Intelligent lighting may create the illusion of occupancy, which is the #1 deterrent for a home break and enter. Smart homes also allow voice activation to emergency services such as calling 9-1-1. The data collected in a smart home can be a rich source of evidentiary data for law enforcement should an incident occur in or near the home. Through the connectivity to the home wireless network, many smart homes devices support remote management and monitoring, which for example, might be used by parents to know when their children are home safely or that someone is at the door.

Challenges to Smart Home Devices

Despite the tangible benefits that have contributed to the widespread adoption of smart home devices, they are not without risks and challenges—especially to personal privacy. Baucas et al. (2021) find that from a cybersecurity perspective, all of these connected devices greatly increase the attack surface (and therefore, the cyber vulnerabilities) that malicious actors may use to intrude on home networks.

Given the volume of personal data that these devices collect—often without the user's knowledge or

consent—there are significant privacy concerns should these devices be compromised. Popular examples of compromises include malicious actors surreptitiously recording audio and video, browser traffic, and more. Given the cyber risks to these devices, there is a need to upgrade hardware, software and firmware regularly.

Many smart home devices are battery-powered, so there is a need to replace batteries in order to maintain the power levels. Plug-in devices may suffer damage (both physical and digital) in the event of a power surge. There is also a need to assure and maintain the device's connectivity to networks, controllers, and/or other devices. Some devices are expensive to purchase and require expertise to install and configure correctly—both initially and over time. Most devices are configured using a smartphone interface, which may pose a challenge to users who are not digitally-literate.

Privacy and Smart Home Devices

From baby monitors to smart TVs to digital assistants/smart speakers, there are devices in your home with the ability to record your personally identifiable information. Whether it is through the recording of information you send/receive/view, or audio/video activity in the home, the potential for *personally identifiable information* (PII) to be collected, stored, and shared by these devices must be addressed. One option to address privacy concerns is to read the cyber hardening guides of these devices (such as this guide from Axis Communications [PDF]), and only buy devices that provide this kind of security documentation.

As you read the guides, educate yourself if the language or steps are not clear. One of the first steps in cyber hardening a device is to ensure that the device's software and firmware are updated. Make sure you only download updates from the manufacturer. Cyber hardening guides may also suggest that you unplug or remove batteries of devices when you are not using them for an extended period.

Another option is to visit sites like Mozilla's *Privacy Not Included* which allow you to search a database of devices known to collect and share private information. Most smart home devices come with accompanying smartphone apps or QR codes linking you to company websites; however, many of these apps and websites will require you to share your personal information—often under the guise of *warranty registration*. Make informed decisions about using these apps and websites, and always confirm the app is not a third party. Many smart home devices require access to your home wireless network, which makes protecting your home's wireless networks a critical step in privacy protection.

Reflection Activity

Celemnti (2021) cites a report released by Hub Entertainment Research which finds that 59% of smart speaker users have privacy concerns. In the article, Clementi quotes David Tice, senior consultant to Hub and co-author of the study, as saying "This new report shows just how pervasive voice control is, and how quickly consumers have embraced it, even if they have major privacy concerns" (para. 5). Voice control has significant benefits as well, so how do you make informed decisions about using smart home devices that support voice commands?

Section 5: Privacy and Home (Wireless) Networks

What is a network? In its simplest form, a network is any two (or more) machines or devices that share data and resources across a medium. Wireless networks, therefore, are networks that rely on *radio frequencies* (RF) and other wireless communication protocols to connect and communicate (send and receive data) between devices. Devices on a home network may be smart devices (called *nodes*) or dedicated networking hardware infrastructure machines such as routers, switches, and controllers. Wired networks are similar to wireless networks in their functions but require physical cables and electrical power. There are many types of home wireless networks and many different protocols that can be used for communication. Examples of wireless technologies include WiFi, ZigBee, Bluetooth, and WiMax. Users can identify a wireless network by its name or *Service Set Identifier* (SSID). Home wireless routers/networks primarily use two frequency bands, 2.4GHz and 5GHz. Both bands have been around for a long time, but the recent emergence of wireless devices that use the 2.4Ghz band has pushed 5Ghz wireless to the forefront.

There are also a variety of network topologies and types of networks that connect your small home network to a much larger network. These larger networks that you connect to can be private (such as your connection to your workplace's corporate network) or public (such as the internet). Networks can be deployed in a variety of designs—each with different advantages and disadvantages. Common designs (also called *layout,* or *topology*) include star, bus, ring, mesh, tree, and hybrid designs. The components of your network depend on the number and types of devices connected to it. For example, you may have nodes (devices) such as computers, laptops, smartphones, controllers, routers, switches, hubs, firewall appliances, a connection medium (wired and/or wireless) and a protocol that regulates how all of these components interact.

The above provides a high-level summary of traditional home networks, but there are other types of networks. For example, satellite communication networks, Cellular communication networks (such as 3G, 4G, 4G LTE, and 5G—the "G" stands for *generation*), and directional radio frequencies (similar to broadcast radio in your car and two–way portable radios). Networks require a connection between a minimum of two computing devices but have no maximum. The largest network in the world is the internet. It is so large that many refer to the internet as a network of networks.

Whether the home network is wired or wireless, Statistics Canada (2021a) reports that 94% of homes in Canada have broadband internet access. This massive adoption speaks to the benefits of internet access—specifically wireless internet. Wireless networks are much cheaper to purchase and faster to deploy than wired networks. Most homes need only a router with a built-in modem to instantly connect to their internet service provider (ISP) such as Rogers, Telus, Bell, and Shaw. Interestingly, these routers that provide the home with wireless connectivity usually require a wired connection—often via a telephone cable or coaxial video cable. Once the router/modem is connected to the ISP, it will support connections—and therefore, internet access—to a multitude of devices within range of the router. A router's range is dependent on several factors; however, an explanation of these factors falls outside the scope of this chapter.

Wireless networks are also more scalable than their wired counterparts and easier to upgrade, making wireless networks more future-proof, which, given the advances in networking technology, makes wireless the preferred option for most homes. The ubiquity and increasing number of smart home devices, wearables, smartphones, and IoT devices that require internet access—many of which do not support a wired connection—make wireless networks the logical choice (pun intended).

Of note is that most smartphones will automatically switch to a known wireless network, which creates significant cost savings to the owner, as cellular data (an alternative to home wireless) is expensive. Lastly, and from a security and privacy standpoint, wireless networks allow for communication on the network to be encrypted and password-protected, whereas, with wired networks, physical access overrides nearly all security measures in place.

Challenges with Wireless Networks

As has been the approach to each of the privacy tools and technologies discussed in this chapter, a discussion on the challenges to wireless networks is appropriate. Despite the significant affordances of wireless networks, there are still risks that need to be considered and addressed. For example, wireless networks are subject to interference with and from other electronic devices. This interference can interrupt or delay data transfer on the wireless network as well as result in incomplete data being received. Wireless networks, especially those on the 2.4Ghz bands, are often competing with other devices on the same frequency—including the microwave,

wireless telephones, and all Bluetooth devices. This makes for a crowded frequency, which is why many home wireless networks offer a 5Ghz connection as an alternative. Many intelligence devices will switch to the faster of the two wireless networks.

Further, wireless networks have range limitations that can create *dead spots* (or locations with low-to-no wireless connectivity) in the home. Also, due to signal leakage outside the walls of the home, wireless is considered by many to be less secure than wired networks as physical access to the devices is not required. This makes it more difficult to secure all nodes on the network. In addition, many homeowners do not take precautions to secure their wireless networks, preferring to leave them as an *open network* for ease of access. Lastly from a security standpoint, given that the wireless network name is configurable, a user can easily connect to a malicious wireless network masquerading as a legitimate one. This is common in restaurants, hotels, and other locations that offer free, open wireless internet.

Privacy and Wireless Networks

Having examined the benefits and challenges of home wireless networks, you may be wondering where this conversation leaves you with respect to securing your private information. Good news! There are a number of strategies and tools to accomplish this.

The first is to leverage the best encryption your wireless controller (or router) supports. The most common wireless encryption protocols are WEP, WPA, WPA2, and WPA3. Of these, WPA3, which was released in 2018, is considered the most secure and is now the standard for all wireless communications due to its use of advanced encryption and session management.

However, WPA3 is not infallible, and vulnerabilities do exist. Consider turning off your home wireless router at night or when you are not at home as a means of reducing the attack surface of your home network. It is also highly recommended that you secure your home wireless network with a complex password and that you change it every 3-6 months. Wireless routers can also be set to not broadcast their SSID (network name), and many privacy and security-conscious homeowners choose this option. This adds a step in connecting new devices, but the security is worth the extra few minutes.

Consider using physical firewall devices or virtual software-based firewalls on your computers and other capable equipment. Set up sub-networks (also called virtual local area networks, or VLANs) for your smart devices as a way to separate them from your other computing devices. When using the internet on those computing devices, use a VPN (discussed in chapter 7 of this e-book) for your day-to-day browsing, banking, and retail purchases. Lastly, if you suspect there might be an issue with an intruder or malicious software

slowing down your wireless network, you can log into the router using your laptop or PC and access the router's configuration pages. These pages will tell you which devices are connected to your network and whether they are consuming your bandwidth.

Reflection Activity

Log into your home router's main configuration page. You may need to do that by typing the router's IP address into your web browser. To find the IP address, you may need to examine the router for stickers or read the documentation that came with the router. Alternatively, you can check online by *Googling* your router's make and model along with the phrase "default IP." You may also find the router's default password (often *admin* or similar). Once you have access, browse to the configuration page that shows all active connections and historical connections. Do you recognize the names of every device in that list? Some of the names may be less clear than others. You will likely see laptops, tablets, smartphones, printers, smart home devices (TVs, video surveillance), and gaming consoles— depending on the devices in your home. Any surprises? Share the results with your peers.

After completing the above exercise, reflect on the scenario below. As you read, consider each of the sections in this chapter and if/how the content of those sections relates or applies to this scenario.

> *Your elderly parents (or grandparents) are not digitally literate and live in a modest home but are concerned about their safety. They want to take advantage of the safety and communication features of smart devices that allow them to alert and get help if they fall or suffer medical distress. Due to arthritis, they have difficulty with buttons and want to use touchscreens and smart devices that support voice commands. They would like you—as a tech-savvy family member—to recommend, purchase, and set up these devices. They also want you to be able to adjust settings and fix issues with these devices from your own home so you won't be inconvenienced whenever they need your technical assistance. What will be your key considerations as you proceed? How will you proceed?*

1. How might the benefits of smart devices and home computing devices outweigh the privacy risks?

2. To what degree does digital literacy impact a person's ability to protect their privacy while also using smart devices?
3. What smart devices are currently being used in your classrooms (or the classrooms of your peers)
4. In what way can smart devices impact the private information of your students?
5. Are you aware of any policies in your workplace that govern the use of smart devices?

Section 6: Future Technologies and their impact on Digital Privacy

Note. Future technology, by J. Sortino, 2017.

This section of the chapter discusses the evolution of the privacy-related tools and technologies discussed in Chapter 6 and Chapter 7 of this e-book. Those chapters discussed current, relevant, and available technologies and services that have matured and been adopted by the consumer market. This section calls on learners to set their eyes on the future of specific digital technologies and see these technologies through the lens of digital privacy. As with the technologies discussed so far, the tools, technologies, systems, and services discussed in this chapter have equal potential to both compromise privacy and PII and to protect it.

This section of the chapter aims to increase your understanding of a number of technologies you may have heard of—and perhaps even studied—in your daily lives. This is accomplished by defining these technologies and examining their role in preserving and compromising your private information. The technologies selected for this part of the chapter are those which stand to have a significant impact on digital privacy. Throughout this chapter, you have encountered words, terms and definitions that were unfamiliar. It is hoped that you have documented these terms in a chart (or other documents) as suggested earlier in this chapter. That list/chart is about to grow! In this section, we discuss and define terms that include

- emerging technology (ET),
- virtual reality,

- augmented reality (AR),
- mixed reality,
- avatar,
- digital (or crypto) currencies,
- Blockchain,
- Drones,
- Robotics,
- Automation,
- quantum computing,
- biometrics, and
- privacy certification.

When you read the words *emerging technology* which images come to mind? Perhaps you imagine technologies from popular media (books, video games, movies, and television) or something else entirely. According to Rotolo et al. (2015), emerging technologies are defined by five attributes: radical novelty, fast growth, coherence, prominent impact, and uncertainty and ambiguity. Mohanad Halaweh (2013) also posits that ET had certain characteristics such as uncertainty, network effect, unseen social and ethical concerns, cost, limitation to particular countries and a lack of investigation and research. Examples of ET include cryptocurrencies, robotics, drones and unmanned aerial vehicles (or UAV), persistent biometrics, human augmentation, quantum computing, nanotechnology, blockchain, augmented and virtual reality, artificial intelligence and machine learning, 5G and 6G wireless networks, and autonomous vehicles just to name a few. Can you think of any other emerging technologies?

Emerging Technology #1: Augmented and Virtual Reality

In this section, we examine the emergence in popularity of augmented reality and virtual reality, and if (or how) the widespread adoption of these technologies may impact your personal privacy. Let's begin by defining these terms. Augmented reality is the superimposition (or overlay) of digital information over a physical space or objects in the real world (Berryman, 2012). Much like virtual reality, the gaming industry—combined with increased adoption and use of mobile devices and networks, provided the lift that augmented reality needed to rise to prominence. Popularized in the 1990s as a tool for jet pilots and astronauts to visualize flight, the first AR-based video games were launched in the early 2000s. A popular example of augmented reality can be found in the *Pokemon Go* mobile app, which launched in 2016 and remains today as one of the top mobile apps for gaming with over 1 billion downloads worldwide (Niantic & Nintendo, 2021). Other factors contributing to augmented reality's meteoric rise come from Hollywood movies, some vehicles, museums, televised sports (e.g., the first down line in NFL games) and a myriad of mobile apps.

At its inception, augmented reality required a *head-mounted display* (HMD) to see the *augmentation* to reality, but this can now be done through glasses, cameras on mobile devices like tablets and smartphones. AR is also popular in education (remote instruction, libraries, etc.) as a tool to allow students to experience places and things—both past and present—and learn about them visually. For example, Google has an app that will allow learners to see animals—including extinct ones—superimposed on the real environment.

Augmented reality is a fascinating technology, but it is often confused with *virtual reality*. According to Berryman (2012), virtual reality is the technology that creates a fully immersive digital or computer-created environment. Whereas AR superimposes digital information on the physical world, VR places you in a fully digital environment—as a substitute for, or replacement of, the real world. In virtual reality, the entire space (and everything in it) is virtual, digital, or a simulation of reality—affording users a full immersion of sensory experience (Jia & Chen, 2017).

While the concept of VR is not new, it is an emerging technology with respect to the adoption and evolution of the uses, markets and educational applications. Similar to AR, VR requires an HMD and other hardware for the users to interact with the virtual environment. In addition to an HMD, VR hardware may include haptic gloves and suits, handheld controllers and cameras in the room to observe and re-create your movements in the virtual space. Haptic gear is especially important to virtual environments as it allows the user to also *feel* (not just see and hear) the virtual world. In essence, advanced virtual reality systems can simulate and stimulate each sensory input.

In addition to gaming, VR has been used in education for years, with research showing increased time on task for learners, motivation, deeper learning, and long-term retention, yet barriers to adoption persist (Kavanagh et al., 2017). In the educational context, VR has been used to enrich the learning environment in many ways. Read the article How VR In Education Will Change How We Learn And Teach for more information on the benefits of immersive 3D learning.

According to Kavanagh et al. (2017), "recently consumer interest in VR has sparked a wide range of new and often crowdfunded virtual reality devices" (p. 104). New VR products are emerging daily, including products like Microsoft HoloLens, Facebook's Oculus Rift/Quest, HTC Vive, Playstation VR (for gaming), and HP Reverb. Similar to AR, much of the resurgence of the popularity of VR has been attributed to the gaming industry (Lindbergh, 2021) but has also migrated to other industries such as health and fitness, retail, and social media.

AR/VR and Privacy

The convergence of VR with social networks has begun. Social networks are an arena where privacy and private information are exchanged freely – often without the user realizing they are doing so (O'Brolcháin et al.,

2016). These technologies present threats to informational privacy, physical privacy, and associational privacy. In learning, *VR Learning Environments* (VRLE) collect private information such as health/body data through sensors, voice patterns, associations, and location data (Gulhane et al., 2019). In VR, recordings of the physical space occupied by a user can also reveal and share private information (Roesner et al., 2014).

Emerging Technology #2: Cryptocurrencies and the Use Of Blockchain Technology

Cryptocurrencies, also called digital currencies, are a form of currency that is a digital artifact (asset). Its value is derived from the use of mathematical algorithms called cryptography. Cryptocurrencies are nearly impossible to counterfeit/duplicate due to the uniqueness of their binary code combined with the tracking of that currency, which uses a companion technology called *blockchain*. Unlike traditional currency, whose value is backed by a central bank or government, cryptocurrencies are decentralized, meaning they are not endorsed, printed, or regulated by an individual entity. Despite the benefits (portability, inflation resistance, divisibility, and transparency), cryptocurrency adoption has been slow—possibly due to the volatility of their value and their association with criminal activity. Bitcoin is the most popular cryptocurrency; other examples include Ethereum, Litecoin, Binance Coin, ZCash, and Tether.

A blockchain is a type of database that stores digital information (data) in *blocks* that are chained together in chronological order (the order they were created). These data can be any kind of information (financial transactions, student grades, medical data, identity credentials, copyrights, voting, supply chain monitoring, loyalty points, or insurance). Like cryptocurrency, blockchain is a decentralized technology (meaning no single group or user has control). It relies on replication/confirmation across many computers to validate, manage, and record transactions (Skiba, 2017). Therefore, a major benefit of blockchain technology is its security. Once entered into the blockchain, records cannot be deleted. All records are immutable (permanent) and viewable by anyone, which plays a significant role in reducing fraud and other criminal activity.

Blockchain in Education

Blockchains can be used to track student progress in a course/program over time and assure the integrity of grades, badges, certificates, academic credentials, and transcripts. It can also be used for file storage for collaborative/group projects, and in the cloud as well. Blockchain can reduce the cost of education by decreasing administrative costs surrounding loans, scholarships, tuition payments, purchasing materials/books, and there are fewer barriers to accessing content. It can reduce administrative costs for libraries as they can track and recover unpaid fines.

Authors and publishers can track how their research is being used while concurrently protecting their

intellectual property. Blockchains can be used to verify and validate student security by confirming their attendance on field trips, buses, and ridesharing. Blockchain also supports the creation of educational marketplaces where students can learn anything from anyone via the blockchain. Lastly, blockchains can be used for tracking the integrity of student assessments and grades (Delgado-von-Eitzen et al., 2021; Black et al., 2019).

Privacy Considerations Of Blockchain Technology

Since one of the most appealing elements of the blockchain is transparency, privacy can be impacted unless data are kept on the blockchain in encrypted form (Alammary et al., 2019). According to Chowdhury et al. (2018), while the process for adding information to the blockchain – and the identity of the author – uses encryption to ensure the integrity of the data, the data/content of the entry is not encrypted. This could lead to private information being shared in the blockchain. Further, due to the nature of blockchain's reliance on public keys, the public key of the blockchain user is visible, which can be an issue if that key type has known vulnerabilities.

Emerging Technology 3: Drones, Robotics, and Automation

Perhaps one of the most well-known but poorly defined terms in digital technology is the word *robot*. Robotics is a field that is often defined by its depiction in popular media, but the actual definition of a *robot* is highly complex (LaFrance, 2016). Depending on the person, this term evokes images of everything from humanoid robots like C3PO in Star Wars to manufacturing robots to robots that vacuum the carpet in your home. In the interest of clarity in this section, let's agree on a definition. A robot is generally defined as any automated machine that executes a specific task, or a number of complex tasks (usually tasks performed by a human) with speed, accuracy, and precision without the need for human intervention. Rather, robots are either controlled externally (e.g., a human or system tells the robot what to do), or internally (e.g., using a combination of sensors and internal programming).

As with the other technologies discussed in this chapter, robotics play a role in education—both as a topic to be learned and as instruments in the learning process. In fact, learning *about* robotics as a field of study has increased in popularity due, in part, to the adoption of STEM programs by many education boards and institutions (Miller & Nourbakhsh, 2016). Learning *with* robots is also on the rise; however, where the robot is supporting the learner directly (e.g., as a simulated teacher) or indirectly (e.g., creating an adaptive simulation like driver training).

Robotics in popular media have been closely linked with *artificial intelligence* (AI) and *machine learning* (ML), resulting in many doomsday depictions of malicious robots and machines causing harm to humans;

however, robotics are being used to support humans in critical ways, including conducting medical surgery, assisting with dangerous or repetitive tasks, and safe driving vehicles. It is important to note that not all *robots* are physical objects. They can also be computer programs or other digital constructs.

The above mention of artificial intelligence and machine learning highlights a critical area for discussion with respect to emerging technologies and digital privacy. While outside the scope of this chapter, other technologies that stand to impact digital privacy in the near future include biometrics—specifically as a primary means of identity presentation and management, human augmentation, or wearable robotics, and quantum computing—which represents the next evolution of the computer. Each of these technologies, and their potential role in preserving or infringing on digital privacy, need to be part of the discussion when considering the horizons of digital privacy.

Passionate about Privacy? Take your privacy knowledge to the next level

The final section of this chapter discusses a few options for those readers who wish to take their privacy knowledge further by earning an industry-recognized certification. One of the most recognized privacy certifications in Canada comes from the *International Association of Privacy Professionals* (IAPP). The certification is called the *Certified Information Privacy Professional/Canada* (or the CIPP/C). According to the IAPP website, the CIPP/C certification is the global standard for people wishing to demonstrate their expertise in privacy laws, regulations and frameworks (n.d.). The IAPP also offers the *Certified Information Privacy Manager* (CIPM) certification, which takes a more management-centric approach that focuses on the operations side of privacy. The *Certified Information Privacy Technologist* (CIPT) certification is geared at those who understand the technological aspects of data protection, privacy, software engineering, IT and information security.

In chapter 5, we discussed the *General Data Protection Regulations* (GDPR), and there is a privacy certification that is GDPR-centric; it's called the PECB Certified Data Protection Officer certificate. According to the PECB (n.d.) website, completion of this certification proves that you possess the professional capabilities and practical knowledge to advise the controller and the processor on how to meet their obligations regarding GDPR compliance.

The *Privacy and Access Council of Canada* (PACC) offers certifications that claim to set the standard of excellence for the data protection profession (n.d.). They offer three privacy certifications of increasing difficulty: the *Associate Access and Privacy Professional* (AAPP), the *Chartered Access and Privacy Professional* (CAPP), and the *Master Access and Privacy Professional* (MAPP). Each of these certifications is valid for three years and requires the holder to complete additional, continuing professional development.

Finally, the *Canadian Institute of Access and Privacy Professionals* (CIAPP) offers an impressive certification called the *Information Access and Protection of Privacy* (IAPP) Certificate. Completion of this certificate program allows the holder to be deemed *CIAPP-certified*. Unlike some competing privacy certification providers who are profit-based, CIAPP is a non-profit organization that claims, "We are not about scaring individuals into becoming certified for any reason other than their own desire to be recognized and support our great profession" (CIAPP, 2021, para. 6).

There are a number of Canadian colleges and universities that offer certificates and courses in privacy protection, privacy management, and other, similar titles. There are also a number of vendor-neutral IT certification organizations that offer data protection certifications, including the *Certified Data Privacy Solutions Engineer* (CDPSE) from ISACA (n.d.) and ISC² offers a privacy certification that is specific to healthcare, called the *HealthCare Information Security and Privacy Practitioner* (HCISPP) certification (n.d.). As you can see, these certifications range from the general to the highly specific depending on the environment and context in which you work.

References

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences, 9*(12), 2400. https://doi.org/https://doi.org/10.3390/app9122400

Alsop, T. (2022, January 10). *Notebook, desktop PC, and tablet shipments worldwide from 2010 to 2025*. Statista. https://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/

Baucas, M. J., Gadsden, S. A., & Spachos, P. (2021). IOT-based Smart Home Device Monitor using private blockchain technology and localization. *IEEE Networking Letters, 3*(2), 52–55. https://doi.org/https://doi.org/10.1109/lnet.2021.3070270

Berryman, D. R. (2012). Augmented reality: A Review. *Medical Reference Services Quarterly, 31*(2), 212–218. https://doi.org/https://doi.org/10.1080/02763869.2012.670604

Black, M., Donelan, L., Higgins, T., Koenig, N., Lenzen, B., Muniz, N., Patel, K., Pfeiffer, A., Taylan, A., Thomas, A., & Wernbacher, T. (2019). From learning to assessment. Utilizing blockchain technologies in gaming environments to secure learning outcomes and test results. *MCAST Journal of Applied Research & Practice, 3*(2), 172–192. https://doi.org/https://doi.org/10.5604/01.3001.0014.4395

Caldwell, A. (2019, February 22). *Technology and fashion unite as the wearable market matures*. Newsroom. https://www.mastercard.com/news/press/2019/february/technology-and-fashion-unite-as-the-wearable-market-matures/

Canadian Access and Privacy Association (CIAPP). (n.d.). *Certification FAQ*. http://www.ciapp.ca/faq%20page.htm

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018). Blockchain versus database: A critical analysis. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1348–1353. https://doi.org/https://doi.org/10.1109/trustcom/bigdatase.2018.00186

Clementi, A. (2020, January 21). *59 per cent of smart speaker users have privacy concerns – report*. Mobile Marketing. https://mobilemarketingmagazine.com/59-per-cent-of-smart-speaker-users-have-privacy-concerns-report-

Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021). Blockchain applications in Education: A systematic literature review. *Applied Sciences, 11*(24), 11811. https://doi.org/https://doi.org/10.3390/app112411811

Dimitrov, I. (2021, March 5). *Invasive apps*. pCloud. https://www.pcloud.com/invasive-apps

Firmbee. (2015, January 20). *Digital devices* [Photograph]. Unsplash. https://unsplash.com/photos/OP2EQ5g-Zkw

Foran, P. (2021, September 24). *Desktop computers make comeback as people continue to work from home*. CTV News. https://toronto.ctvnews.ca/desktop-computers-make-comeback-as-people-continue-to-work-from-home-1.5599828

Gartner, Inc. (2016, December 07). *Gartner survey shows wearable devices need to be more useful.* https://www.gartner.com/en/newsroom/press-releases/2016-12-07-gartner-survey-shows-wearable-devices-need-to-be-more-useful

Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., & Hoque, K. A. (2019). Security, privacy and safety risk assessment for Virtual Reality Learning Environment Applications. *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1–9. https://doi.org/10.1109/ccnc.2019.8651847

Halaweh, M. (2013). Emerging technology: What is it?. *Journal of Technology Management & Innovation, 8*(3), 19–20. https://doi.org/http://dx.doi.org/10.4067/S0718-27242013000400010

Holzhauer, B. (2020, October 22). *The pandemic is fast forwarding us to a cashless society—and making life harder for the unbanked*. Forbes. https://www.forbes.com/sites/advisor/2020/10/22/the-pandemic-is-fast-forwarding-us-to-a-cashless-society-and-making-life-harder-for-the-unbanked/?sh=1a5bbec7f1fb

International Association of Privacy Professionals (IAPP). (n.d.). *The value of certification*. https://iapp.org/certify/

ISACA. (n.d.). *Validate your expertise. Boost your IT profile*. https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer

(ISC)², Inc. (n.d.). *HCISPP – The HealthCare Security Certification*. https://www.isc2.org/Certifications/HCISPP

Jia, J., & Chen, W. (2017). The ethical dilemmas of virtual reality application in entertainment. *22017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC),* 696-699. https://doi.org/https://doi.org/10.1109/cse-euc.2017.134

Kavanagh, S., Luxton-Reilly, A., Wuensche, B., & Plimmer, B. (2017). A systematic review of Virtual Reality in education. *Themes in Science & Technology Education, 10*(2), 85–119. https://doi.org/https://files.eric.ed.gov/fulltext/EJ1165633.pdf

Klosowski, T. (2021, May 6). *We checked 250 iPhone apps—this is how they're tracking you*. Wirecutter Inc. https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/

LaFrance, A. (2016, March 22). *What is a robot?*. The Atlantic. https://www.theatlantic.com/technology/archive/2016/03/what-is-a-human/473166

LeFebvre, D. (2018, December 19). *Digital thermostat* [Photograph]. Unsplash. https://unsplash.com/photos/RFAHj4tI37Y

Lindbergh, B. (2021, January 12). *Waiting for the future of virtual reality*. The Ringer. https://www.theringer.com/2021/1/12/22226387/virtual-reality-playstation-xbox-oculus

Market Research Engine. (2021, February 11). *Wearable devices market research report (report ID: SEWDM717)*. https://www.marketresearchengine.com/wearable-devices-market?mod=article_inline

Mehdi, Y. (2020, March 16). *Windows 10: Powering the world with 1 billion monthly active devices.* Windows Experience Blog. https://blogs.windows.com/windowsexperience/2020/03/16/windows-10-powering-the-world-with-1-billion-monthly-active-devices/

McKeon, J. (2021, September 1). *61M Fitbit, Apple users had data exposed in wearable device data breach*. Patient Privacy News. https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach

Mikalauskas, E. (2021, March 17). *Android apps are asking for too many dangerous permissions. Here's how we know*. CyberNews. https://cybernews.com/privacy/android-apps-are-asking-for-too-many-dangerous-permissions-heres-how-we-know/

Miller D.P., Nourbakhsh I. (2016) Robotics for education. In B. Siciliano, & O. Khatib (Eds.), *Springer handbook of robotics* (pp. 2115-2134). Springer, Cham. https://doi.org/10.1007/978-3-319-32552-1_79

Niantic Inc., & Nintendo/Creatures Inc./GAME FREAK Inc. (2021). *Pokémon GO* [Mobile App]. Apple App Store. https://apps.apple.com/us/app/pok%C3%A9mon-go/id1094591345

Office of the Privacy Commissioner of Canada. (2020, August 20). *Smart devices and your privacy*. https://www.priv.gc.ca/en/privacy-topics/technology/02_05_d_72_iot/

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2015). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Science and Engineering Ethics, 22*(1), 1–29. https://doi.org/https://doi.org/10.1007/s11948-014-9621-1

Paus, L. (2018, May 2). *Wi-Fi or Ethernet: Which is faster and which is safer?.* WeLiveSecurity. https://www.welivesecurity.com/2018/05/02/wifi-ethernet-faster-safer/

Pew Research Center. (2015, March 19). *Internet seen as positive influence on education but negative on morality in emerging and developing nations*. https://www.pewresearch.org/global/2015/03/19/1-communications-technology-in-emerging-and-developing-nations/

Pew Research Center. (2017, May 25). *A third of Americans live in a household with three or more smartphones*. https://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/

Privacy & Access Council of Canada (PACC). (n.d.). *Certification*. https://pacc-ccap.ca/certification/?cn-reloaded=1

Privacy Rights Clearinghouse. (2017, December 19). *Smartphone privacy*. https://privacyrights.org/consumer-guides/smartphone-privacy

Professional Evaluation and Certification Board (PECB). (n.d.). *GDPR – Certified Data Protection Officer*. https://pecb.com/en/education-and-certification-for-individuals/gdpr/certified-data-protection-officer

Qashlan, A., Nanda, P., He, X., & Mohanty, M. (2021). Privacy-preserving mechanism in smart home using blockchain. *IEEE Access, 9, 103651–103669*. https://doi.org/https://doi.org/10.1109/ACCESS.2021.3098795

Roesner, F., Kohno, T., & Molnar, D. (2014). Security and privacy for Augmented Reality Systems. *Communications of the ACM, 57*(4), 88–96. https://doi.org/https://doi-org.uproxy.library.dc-uoit.ca/10.1145/2580723.2580730

Rotolo, D., Hicks, D., & Martin, B. (2015). What is an emerging technology? *Research Policy, 44*(10), 1827–1843. https://doi.org/https://doi.org/10.1016/j.respol.2015.06.006

Shaabana, N. (2019, March 01). *Smartwatch* [Photograph]. Unsplash. https://unsplash.com/photos/m7K2P1cIf2c

Sortino, J. (2017, February 27). *Future technology* [Photgraph]. Unsplash. https://unsplash.com/photos/LqKhnDzSF-8

Skiba, D. J. (2017). The potential of blockchain in education and health care. *Nursing Education Perspectives, 38*(4), 220–221. https://doi.org/https://doi.org/10.1097/01.nep.0000000000000190

Statistics Canada. (2021a, May 31). *Access to the internet in Canada, 2020*. https://www150.statcan.gc.ca/n1/daily-quotidien/210531/dq210531d-eng.htm

Statistics Canada. (2021b, September 29). *Canada's population estimates: Age and sex, July 1, 2021*. https://www150.statcan.gc.ca/n1/daily-quotidien/210929/dq210929d-eng.htm

United States Census Bureau. (2021, October 08). *Computer and internet use in the United States: 2018*. https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html

Witkowski, W. (2022, January 15). *The pandemic PC boom gave personal computers their biggest year in nearly a decade*. MarketWatch. https://www.marketwatch.com/story/the-pandemic-pc-boom-gave-personal-computers-their-biggest-year-in-nearly-a-decade-11642013463

9.

DIGITAL PRIVACY LEADERSHIP

Bill Muirhead and Lorayne Robertson

New challenges for educational leaders

Addressing digital privacy within educational settings requires new skills and new leadership qualities to support learning without the risk of privacy infringements. Leaders must ensure that learning environments are managed in ways that protect student privacy and can avoid unintended risks when adopting new technologies including student information systems and student and teacher software and hardware. There is growing awareness of the responsibilities of managing privacy within learning contexts. As Nagel (2018) observes from an analysis of the *Speak Up Research Project for Digital Learning*, "Data privacy and security are top concerns among education IT pros. More than half of technology leaders in K-12 schools (58 percent) report their top concern with cloud applications is ensuring data privacy" (p. 34). Given this significant anxiety among school leaders regarding privacy in general and cloud computing applications in particular, there has been insufficient research and attention toward identifying what can best be called *leading through privacy risk*.

Within educational settings, a number of technological innovations and their growing use within schooling have accelerated, highlighting the challenges that educational leaders face in managing emerging privacy concerns. The challenges faced by educators can be broadly grouped into the following categories:

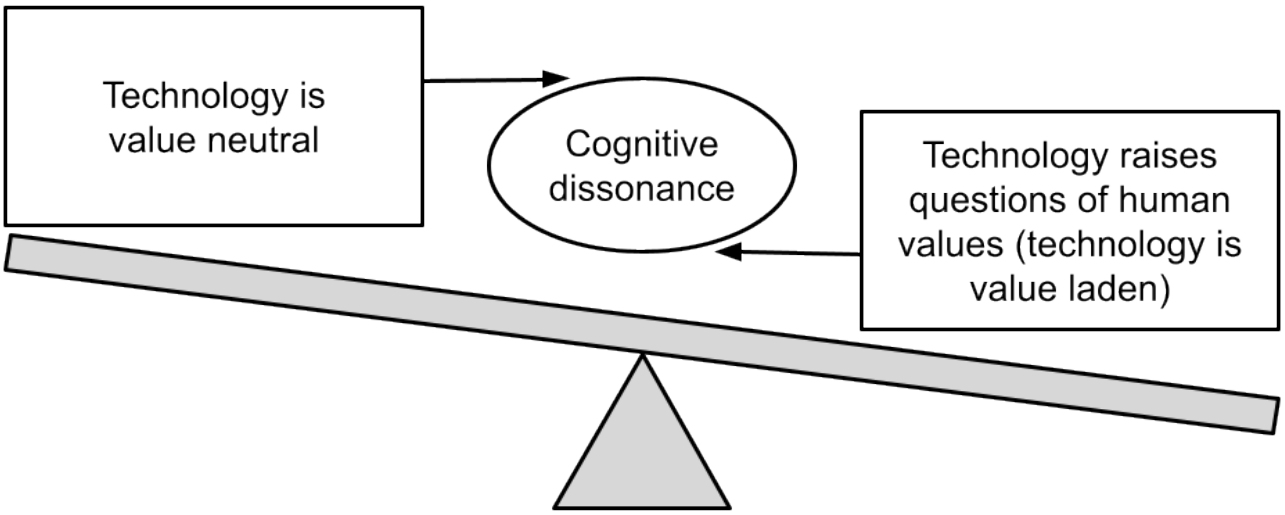
1. Digitization and collection of student data, including digital permanence
2. The leadership gap informed by both education and technological skill sets
3. The leadership matrix
4. Adoption of cloud-based applications which provide both convenience and risk
5. Leadership responses to curricular gaps regarding privacy education

In an attempt to conceptualize how to balance convenience against protection (the privacy paradox), educational leaders are advised, as a first step, to consider their own personal and professional values that inform technological adoption and leadership actions. Rather than taking an applied view of technology as

solutions in search of problems, the authors argue that educators and technology leaders must first take a step back to construct a philosophical perspective regarding the complex roles and changes to an organizational culture that technology plays within organizational operations. Leaders must also consider the potential effects that new affordances can have on learning environments. Mastering the cognitive dissonance inherent in the use of educational technologies is depicted as a fulcrum balancing technological affordances as value-neutral with values-based beliefs (Webster, 2017). Identifying one's beliefs is a crucial first step in identifying the need for student privacy while balancing new technological capabilities. Figure 1 below from Webster (2017) highlights the intellectual work required of technology leaders to inform their actions regarding privacy.

Figure 1.

Technology is value-neutral vs. technology raises questions of human values



Identifying one's personal beliefs about privacy is a crucial leadership step before leading systems in the use and application of student data and its potential learning benefits. Basing decisions on personal beliefs will help leaders weigh potential risks associated with data acquisition and aggregation and with institutional requirements and potential privacy implications.

Digitization and the collection of student data

Dataism is a term articulated by David Brooks in 2013 in an article from the New York Times where he described a dataism mindset that, if it could be measured it should be collected and used to quantify and inform the human experience. Quantification of the human experience through a combination of technologies

that can capture, store and enable analytic tools to identify trends, and insights have been a major development in computing over the past two decades. Lupton (2021) conducted a study of Australian teachers' understanding and practices surrounding the digitization of student data. She observed that *students'* learning, physical movements and other personal details have been the subject of intensifying forms of monitoring, measuring and algorithmic processing with the use of educational technology" (p. 281). Jim Balsillie (2019), the co-founder of the Blackberry and President of Research in Motion has observed, in The Financial Post, that the present domestic and global regulatory frameworks are not designed to deal with emerging challenges such as disinformation, fake news, the toxicity of social media, the dynamics of the attention economy, and the technology's power through the control of data. He states that "data is not the new oil-it's the new plutonium" (Balsillie, 2019, para. 9). He further observes that data can be both powerful but when misused it can be difficult to clean up. He advocates for international coordination to manage data.

Yet, while digital student information is increasingly stored and retained over time in data sets (known as digital permanence or digital legacy), concerns regarding student privacy and digitalization of student data have grown. Unlike past practices where student information was paper-based and information about each student was kept in administrative offices or archived in school board basements in corridors filled with file boxes, the development of inexpensive computer storage and interconnected computer networks has meant that student achievement data, student personal information, teacher-generated data, student assignments and projects, test scores, specific family data including siblings, addresses, demographic data and historical data can now be both kept inexpensively and shared widely among a wide set of school personnel in a context where privacy policies are underdeveloped. While digitized student information may assist educators to better identify learning interventions or create new approaches to support learners with specific needs, widespread access to student data and the potential to misrepresent student capabilities can lead to misdirection at best and, at worst, reinforce prejudices and labelling of marginalized students. As Chapter 6 on the Privacy Paradox highlights, the ever-increasing digitalization of the human experience creates privacy issues for many and particularly students for whom consent is not given, asked for, or fully understood.

For educational leaders it is an essential task to protect student data as the digitization of student data now include:

- Student assessments
- Teacher notes
- Clinical records
- Family composition

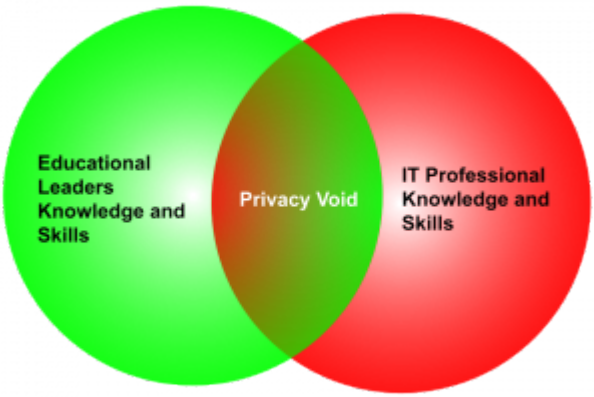
- Family income
- Ethnicity
- School attendance

And, potentially:

- Health records
- Court records

Understanding how data is collected, aggregated, and to what purposes it is used is a crucial leadership requirement to leaders in educational settings.

The Leadership Gap



The requirement to consider privacy within educational systems can lead to privacy avoidance where privacy policies and consequent decisions are avoided for lack of expertise or avoidance of complexity. This void often leaves front-line educators to *figure it out* on their own or to interpret policies without the skills or foundational knowledge. The consequence can often be, a) to avoid digital technologies or minimize their use in educational settings, b) avoid any innovative use of digital technologies for fear of inadvertently breaching system policies or creating privacy risks or c) utilizing new technologies without consideration of personal or family privacy risks or d) adopting new technologies believing all care has been taken but where risks remain because of skill deficits or because the expertise is unavailable. For example, when adopting a new cloud-based application for learning, consideration may be given to secure consent from parents and perhaps students with due care to data retention. Or consideration surrounding cloud security may be considered without concern about local network security or local authentication (password management). Another option is to secure the data through an agreement with the cloud-based service provider.

A central leadership task for system leaders is to support personnel to acquire both high-level instructional skills while also acquiring technological knowledge to inform and lead the use of learning technologies. The

different career paths and formal education followed by educators and computer science professionals often lead to perspectives that are domain-specific and omit a holistic view of issues facing educators when addressing privacy issues in school systems. The figure above outlines the overlapping and complementary skill sets required in an increasingly digitized learning environment. Consequently, one of the central questions within educational settings is to answer the question,

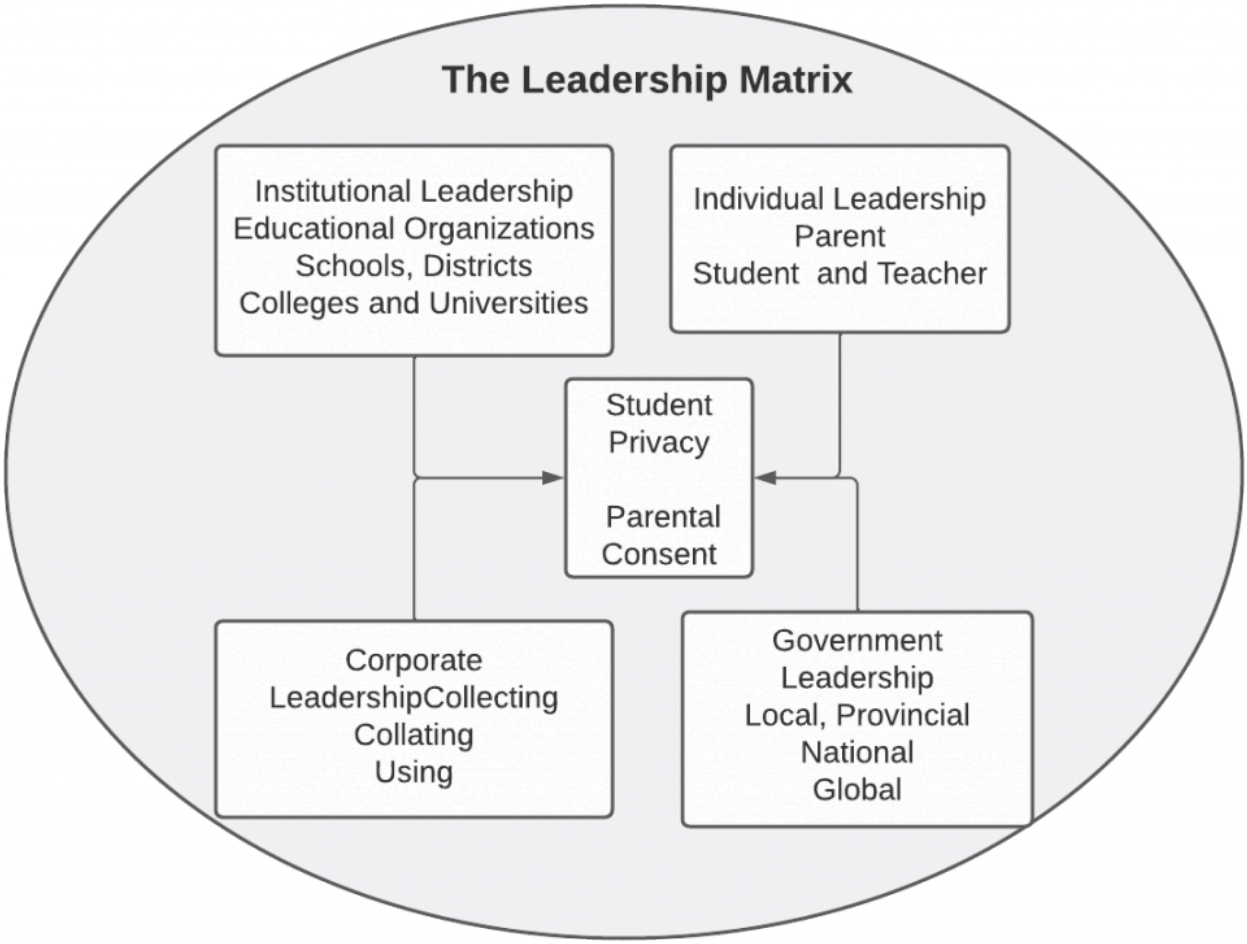
> How can educational systems support leaders to acquire both deep technological skills while also possessing educational competencies that can help leaders answer the following questions from a variety of perspectives.
>
> - What does privacy mean in educational settings?
> - What are the leadership tasks required to address protecting student privacy?
> - How do educational leaders ensure the collection and retention of student data is thoughtful and time-limited?
> - What tasks are required to develop and ensure privacy concerns are embedded across schooling curriculums?

The Leadership Matrix

Educational leaders already operate in a complex environment where considerations about privacy are diverse and multi-faceted. Teachers may view privacy through a lens of how best to support student achievement, believing that systems or school administration are best able to *manage* privacy concerns and specific privacy settings. Administrators can view privacy through a lens of *risk* avoidance where restricting the potential use of particular classroom tools is often considered key. Parents, on the other hand, view privacy through a lens of concern for their children but cede their concerns to school systems through trusting educators to protect their children from harm. Finally, students are often the last to be consulted, if at all, and may have a curriculum that is silent on the concepts of consent and privacy when using digital technologies. A consequence of this diverse set of beliefs is that privacy is considered important but the responsibility for privacy is left to *others* to manage.

Figure 2.

The Leadership Matrix.



In the *Digital Privacy: Leadership and Policy course*, the authors have discussed the complexity of privacy responsibilities, the privacy paradox and the growing use of artificial intelligence and machine learning, the use of mobile devices, digital surveillance, the complexity of policies for regulating student privacy and the real potential for the misuse of personal information. Yet, the roles and responsibilities of educational leaders and other actors within schooling settings regarding protecting student privacy and misuse of student data remain less well examined in the academic and professional literature. Schrum and Levin (2015) write that, while school or district leaders cannot be expected to do everything alone, they must think systemically and utilize *skills and strategies of distributed leadership* to engage others and create a shared vision for technologies in schools. As members of the course authorship team, we hope to raise awareness of privacy as a vital component of technology adoption and use. The leadership challenge of consultation with many players while attempting to create consensus around issues that are sometimes at odds with other beliefs has only compounded the necessity to conceptualize the leadership matrix (Figure 2) where student privacy and safety is

both an educational issue and a societal one. While boundary issues abound when considering student privacy, the leadership challenge is to acknowledge boundary issues and manage that which is within the scope of school administrators.

Cloud-Based Applications: Convenience and Risk

The requirement to provide leadership about privacy has never been more acute for educational leaders. The emergence of a global pandemic in 2019 and the subsequent closing of schools and the move to embracing online learning and/or learning from home has resulted in education moving from the school and classroom to the virtual classroom. The recent pivot to learning online throughout the global pandemic has only highlighted the complex issues and problems of protecting student privacy in online and learning at home settings. Moving from a face-to-face environment to an online environment has often resulted in the additional and inappropriate collection of children's personal information. Han (2020) observes that, while many online teaching platforms are depicted as transactional in nature to facilitate interactions and learning online, the collection of student information and potential collection of student presence through video screen recording, screen capture and chat archiving presents serious concerns for privacy and how to protect children from privacy risks.

This was echoed by the 2020 report from the Organization for Economic Co-Operation and Development concerning the effect of Covid 19 on children (Thevenon & Adema, 2020) which pointed out that the pivot to online learning presented unique challenges regarding data collection and retention of personal information used to access and monitor student engagement in online activities. Online learning and the facilitation of learning through Internet activities only intensified the difficulties faced by school leaders when consulting with the myriad actors and intersecting policies that required consideration. This pivot to online learning was enabled by the use of online digital tools and in some cases the distribution of computing hardware and software to students at home. From Zoom classes to Google Classroom, Microsoft Teams, Edsby, and Emodo Canvas, school districts embraced new tools to organize and continue education at home. Additionally, tools such as PearDeck, Storybird, Kahoot! and Class Dojo, among many others, emerged as instructional, communication or companions to school learning management systems. But with the pivot to learning online, so too came questions about how to manage student privacy, how best to manage student login information, how to document learning and the associated learning activity record, and how to document students' learning. The shift to online also heightened the need to identify which policies should be developed to guard against the over-capture of student data as well as its retention.

Leadership Responses Privacy Gaps in Curriculum Policies

Note. Lighthouse starry night, by N. Jennings, 2021.

Educators wishing to provide leadership on issues concerning student privacy and safe Internet usage involve not only administrative competence but curricular leadership to support student empowerment to make informed choices about personal safety online. The inclusion of privacy across the curriculum includes a recognition that protecting students' privacy is an ethical concern. Choice is not only about asking for consent but asking again and again. This becomes more difficult in an era of persuasive technology. Smids (2012) gives the example of the sound made by the car if anyone does not fasten their seat belt. The continuous sound is a persuasive technology and also a coercive technology. A persuasive technology that allows voluntariness would be the example where the seat belt reminder rings once or twice and then stop without compelling someone to put their seat belt on. Smids (2012) suggests an ethical requirement of *voluntarism* is that it should be intentional, free from controlling influences, and is an informed decision. It requires leadership to make certain that voluntariness is part of informed consent and that this applies to all online learning applications.

Teachers, students, families, staff all share concerns about individual privacy and the trust that their online actions are free from privacy risks. Educational leaders bear a responsibility to support the development of resources to support educating students about privacy risks and their online presence. Moon (2018) observes that,

> Students lack the knowledge they require to participate safely in a digital world creating a gap in understanding. Access to knowledge is required to foster understanding and create informed students that have learned the skills they will need to navigate the potential harms of digital access. (p. 292)

Curricular leadership involves not just ensuring resources are available but actively involving oneself as a leader in multiple ways:

- Ensuring curricula align with provincial outcomes where available,
- Establishing frameworks to measure goals while establishing timelines for assessing progress,
- Ensuring that curriculum resources are age and stage appropriate,
- Assisting in identifying cross-curricular approaches to privacy and safe internet use,

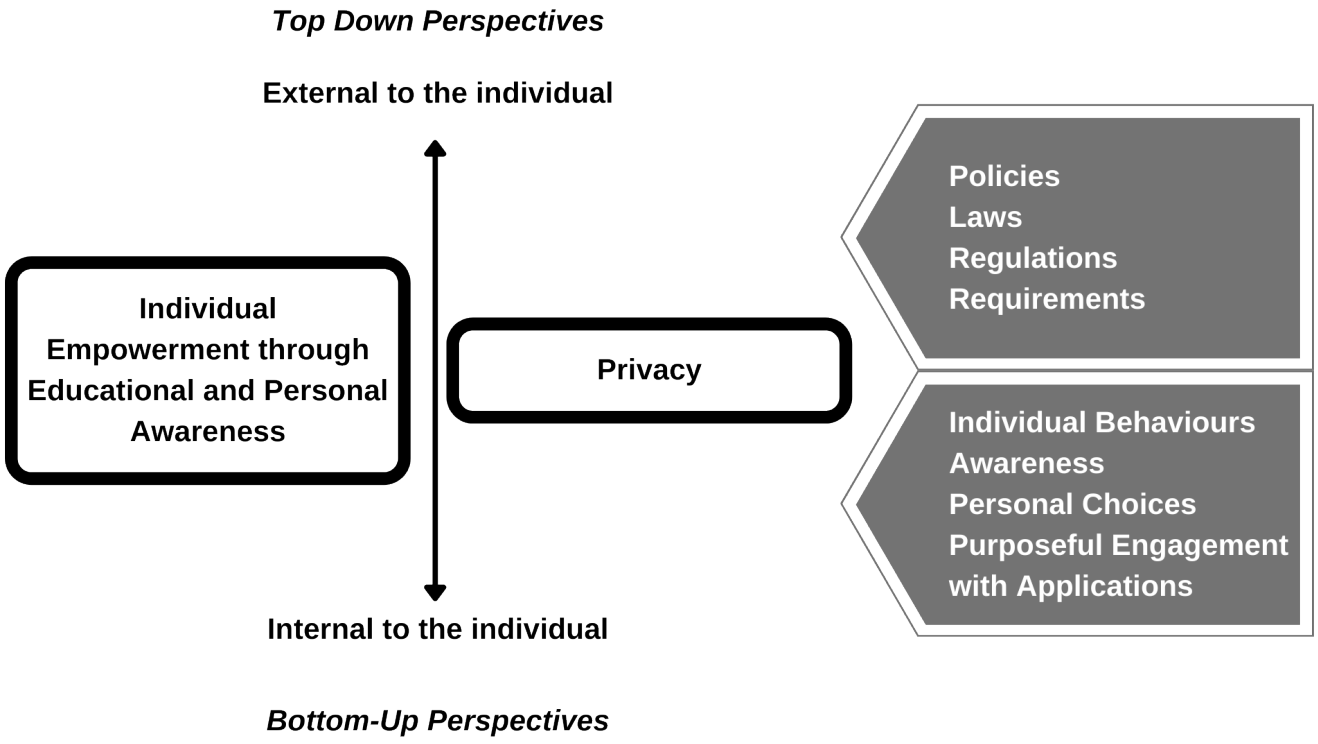
- Ensuring that the school systems values are embedded and reflected in all aspects of curricula, and
- Supporting students and families from across diverse backgrounds.

Curriculum policies must not only be a checklist of do's and don'ts but also includes giving students the knowledge to avoid harm, challenging what appropriate online behaviours are expected, internet safety and considerations about the use of social media including awareness about and how to respond to inappropriate invitations, solicitations and grooming online. The curriculum can include discussions about responsible online use, school codes of conduct and acceptable use policies.

Examples of topics to be included in privacy-focused curricula include topics and concepts about a) greeting a healthy balance between online and offline behaviours b) how to engage in online activities from an ethical base of understanding risk, consequences while understanding others, c) making purposeful choices to protect personal information about oneself and others, d) building healthy relationships online and e) developing good habits and understandings about hardware settings to address online security. More specifically, topics such as public Wi-Fi risks, gaming and online security, passwords and their use, recognizing and managing phishing and spam, how to read terms of service when using cloud-based applications and how to circumvent flirting and sexting overtures online.

Figure 3.

Top down and bottom-up perspectives.



To help leaders to conceptualize learning outcomes for privacy initiatives in a post-digital age, the authors debated what it meant to be *private* and how to understand the push and pull of being a digital citizen in today's world. If the goal of privacy is to enable everyone to engage with the rich experiences that digital technologies can offer and the interconnectedness with persons, services and resources online that the Internet has to offer, it is essential to empower everyone (most especially children) about how to protect and secure one's self in an environment where the privacy paradox, the legislative environment, monetization of online behaviours and trans-generational views about digital citizenship are under development and shaped by past and current experiences. In trying to understand the role of educators and what leadership they can offer to a world in flux, we settled on the overarching goal of *empowering young people* to be aware of changes around them and inspire them to make purposeful decisions about how they will live their lives now and into the future. The figure offers a sense of both top-down efforts to protect and create proactive actions to protect privacy while concurrently efforts to empower and educate children about their own privacy actions to make personal choices about engaging in the online world in which they now live, will work and will occupy throughout their lives. Just as the digital/online world will comprise the present and future so too with concerns about privacy. The answer, therefore, is to educate and empower the citizens (students) for the future.

Recommendations for Educational Leaders

We offer the following recommendations in support of more privacy-conscious learning environments. The recommendations are not comprehensive; they are a first step in addressing the leadership gap regarding privacy considerations in education.

1. Leaders must embrace a privacy orientation across all operations and learning contexts to ensure not only compliance with existing policies and laws but also to ensure that privacy is at the forefront of teaching and learning.
2. Leaders must ensure they possess or ensure they can acquire technological knowledge and skills in areas of privacy and security to complement their experience as educators
3. Leaders must designate a single point of contact to ensure privacy is not an afterthought but is a designated/defined responsibility within educational operations.
4. Leaders must support the creation of an annual privacy report including reporting on privacy breaches and ongoing privacy risks.
5. Leaders must engage with all those with whom the educational enterprise touches to ensure that information about and decisions about privacy risk abatement are communicated.
6. Leaders must ensure that privacy concerns, required actions and exploring privacy values are embedded across curriculum policies with age-appropriate resources to support front-line educators.
7. Leaders must ensure that consent for technological services is updated and that asking for consent once

is not informed consent.

8. Leaders must establish policies regarding data access and data retention across all educational operations.
9. Leaders are encouraged to reflect on technological use and the values inherent in the adoption of emerging technologies with specific attention to technologies associated with school safety and surveillance.
10. Leaders must ensure that digital citizenship efforts equip students to be proactive versus reactive when managing their presence and behaviour on the Internet.

Some Closing Thoughts

Educators in the present era find themselves within a vortex of rapid technology innovation. It is also a time of significant social disruption. This is happening not only for health concerns but as technology enables the disclosure of crimes against humanity as they occur in real-time, and as they are unearthed from the past. Technology has also enabled the voices of those who have been at the margins of society and seek their rightful membership in society.

At the heart of all educational endeavours, educators hold the safety, security and well-being of the students who have been entrusted to them for education, as well as the students who have chosen their educational institution. These students will need the skills to solve problems during times of great complexity and innovation. Digital privacy is one of those messy, authentic problems of progress. As leaders work toward solutions, they need to model the skills advocated in this online course: ethical problem-solving; knowledge sharing and knowledge building through communication and collaboration; and decision-making guided by critical, reflective practice.

We invite the instructors and students who take the Digital Privacy course to contribute case studies and examples in Chapter 10. This will help to evergreen the course and provide sector-specific examples of authentic digital privacy case studies.

References

Balsillie, J. (2019, May 28). *Jim Balsillie: 'Data is not the new oil – it's the new plutonium'*. Financial Post. https://financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium

Brooks, D. (2013, February 05). *The philosophy of data*. The New York Times. https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html

Han, H. J. (2020). *As schools close over coronavirus, protect kids' privacy in online learning*. Human Rights Watch. https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning

Moon, E. C. (2018). Teaching students out of harm's way. *Journal of Information, Communication & Ethics in Society, 16*(3), 290–302. https://doi.org/10.1108/JICES-02-2018-0012

Jennings, N. (2021, January 07). *Lighthouse starry night* [Photograph]. Unsplash. https://unsplash.com/photos/VsPsf4F5Pi0

Nagel, D. (2018). Student data privacy a top concern of K-12 tech leaders. *THE (Technological Horizons In Education) Journal, 45*(4), 34. https://digital.1105media.com/THEJournal/2018/THE_1810/TJ_1810Q1.html#p=34

Schrum, L., & Levin, B. B. (2016). Educational technologies and twenty-first-century leadership for learning. *International Journal of Leadership in Education, 19*(1), 17-39. https://doi.org/10.1080/13603124.2015.1096078

Smids, J. (2012). The voluntariness of persuasive technology. In M. Bang, & E. L. Ragnemalm (Eds.), *International Conference on Persuasive Technology: Persuasive technology, design for health and safety* (pp. 123–132). Springer. https://doi.org/10.1007/978-3-642-31037-9_11

Thevenon, O., & Adema, W. (2020, August 11). *Combatting COVID-19's effect on children*. Organisation for Economic Co-Operation and Development. https://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-s-effect-on-children-2e1f3b2f/

Webster, M. D. (2017). Philosophy of technology assumptions in educational technology Leadership. *Educational Technology & Society, 20*(1), 25–36. https://www.jstor.org/stable/jeductechsoci.20.1.25

10.

CASE STUDY: PROTECTING CHILDREN'S PRIVATE INFORMATION IN EARLY CHILDHOOD PROGRAMS

Protecting Children's Private Information in Early Childhood Programs

Enas Zaghloul; Angela Walsh; Roohi Jawad; Evelynn Jacob; and Kalaivani Sritharan

In this chapter, we outline a case study that includes:

1. Context
2. The Policy Environment
3. People and Organizations
4. Problem definition
5. Solutions
6. Reflection on the Solutions
7. Discussion Questions
8. Video

Executive Summary

Parents using child care may appreciate the convenience of an app to communicate with their daycare but also may need to realize who has access to the information about their child via the app. Similarly, teachers may share information with parents through an education app but not realize who has access to the shared information. This case study describes one such scenario.

Child care providers (CCP) in Ontario are regulated and provide services for children ages birth through 12 years. The Ontario Ministry of Education is responsible for child care overall and gives full-day kindergarten to all four and five-year-old children. Child care is also provided for out-of-school hours and for children who are not yet school-aged.

While companies have designed educational apps to simplify communication with parents, some apps share families' personally-identifiable information (PII; Bradshaw et al., 2013), making it challenging for CCPs to communicate effectively with children's families while simultaneously guarding the PII of students and parents. This precarious situation is augmented if the education app's providers experience privacy breaches.

The authors of this case study are experienced educators guided by insight from Warren and Brandeis (1890) that families and children have a right to privacy "in its fullness" (p. 213). Throughout this chapter, we explore the present policy environment and the roles and challenges of protecting privacy for CCPs and families using educational applications. The authors ultimately propose various problem solutions and reflect on their efficacy.

Context

Edmodo, a popular communication tool for K-12 teachers, began in 2008 as an open-source learning management system. According to the official website for the State of Vermont (2022), Edmodo offered lesson planning tools, live classes for synchronous delivery and the opportunity to hold classes in "enclosed communities." Edmodo quickly became popular with teachers; Edmodo has claimed to have 90 million users in 400,000 schools in 192 countries (Corcoran & Wan, 2018). When schools or childcare providers (CCPs) outsource communication to a company like Edmodo, they outsource more than the platform. Parents, students, participating schools, and CCPs also share private information. Regulations regarding "who owns the data" may not be apparent to everyone involved.

Edmodo was hacked in May 2017, leading to a report that tens of millions of users' account names and email addresses were for sale on the dark web (Klose et al., 2020; Herold, 2017). Edmodo was responsible for informing users and regulators of a data breach. Subsequently, Netdragon acquired the EdTech platform in 2018 (Corcoran & Wan, 2018). In 2022, Edmodo ceased to operate, leading experts to question what would happen to the large amounts (ten years) of sensitive data stored in Edmodo from participating schools, CCP and families. Fortunately for educators, parents and students, Edmodo has indicated that it intends to destroy the data it holds (Mollenkamp, 2022).

The Policy Environment

Although policies for privacy protection for students are advancing, many current education apps still allow unauthorized access to PII. There is, in addition, a lack of privacy protection laws internationally. The Global Privacy Enforcement Network of 60 global privacy regulators raised the alarm for protecting student and family PII based on their findings that many internet-based education applications require learners and

students to submit PII, including emails, to access their services (GPEN, 2017). Some information security policies designed to protect the PII of students and families are beginning to be implemented globally, such as the European Parliament's. (2016) General Data Protection Regulation (GDPR) which protects European students.

The policy is a planned response, but Cavoukian (2011) asserts that the privacy policies of most online platforms are reactive. Durrani and Alphonso (2022) examined data and findings from the Humans Rights Watch (HRW) concerning the abrupt shift to online learning at the onset of the COVID-19 pandemic. They found that students' information from EdTech apps was shared with advertisers, reaffirming global privacy and safety gaps in educational technology (Durrani & Alphonso, 2022). In a survey of 3084 US students, 52% said that they have been "very/somewhat concerned" with sharing their data, including COVID-19 vaccination information, and 56% were concerned about data breaches such as being "zoom-bombed" by uninvited users interrupting their online classes (Klein, 2021).

According to Bradshaw et al. (2013), because educational apps require users to enter PII for the child and family, Canadian legislation needs to improve digital privacy protection for young children, mainly since more digital education solutions have emerged during the COVID-19 pandemic. In Canada, the House of Commons (2019) Personal Information Protection and Electronic Documents Act is in place for monitoring the commercial use of information federally. However, education is the responsibility of the provinces, thus creating overlapping policy issues and gaps. There also exists a gap in curriculum policy evidenced by the lack of incorporation of essential learning concepts of digital privacy, including digital permanence, digital footprint, and digital dossier, across Canadian curriculum policies (Leatham, 2017)

Within Ontario, CCPs must comply with the Child Care and Early Years Act (CCEYA, 2014) legislation and the Municipal Freedom of Information and Privacy Act (MFIPPA, 1990) which is the overarching protection of information legislation that provides more detail on protecting and securing PII. Though MFIPPA predates widely used digital platforms and offers the definition that "personal information is inclusive of age, race, origin, identifying symbol or number, and unique physical characteristics, among others, that can be used to identify an individual" (s.2-1(a)). Although MFIPPA is yet to be updated to reflect a digital environment, it acknowledges that a record of PII includes electronic information s.2(1). MFIPPA is essential in protecting learners because it prohibits institutions, including schools, from the unconsented use of stored personal information (Bradshaw et al., 2013).

The United States began protecting student privacy as early as 1974 under the Family Education Rights & Privacy Act (FERPA). More recently, in response to the increase in the use of the internet and digital applications, they enacted the Children's Online Privacy Protection Act (COPPA, 1998) and the Children's Internet Protection Act (Federal Communications Commission, 2003) to protect children's privacy (Poggi, 2021). FERPA (1974) outlines the requirements to protect PII, while COPPA (1998) establishes the age of 13 for consent for an online profile. These laws can serve as an example in identifying the type of records and

sensitive information that should be protected when uploaded to digital applications. Even though multiple layers of legislation can be cumbersome, Flanigan (2015) argues that enacting vast bills at the federal and state level is essential in enhancing children's data privacy. However, there is a lack of teacher training around them.

The European General Data Protection Regulation (GDPR, 2016) Article 4 identifies:

> 'personal data' as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (p.33)

According to the office of the Privacy Commissioner of Canada (OPC), the GDPR protects the transfer of PII under Article 46, which states that if an organization has appropriate safeguards, it can transfer data to other countries without authorization from a supervisory authority within the EU (OPC, 2020). While this only applies to any organization doing business with Europe, it protects students' privacy and might benefit the global use of educational apps. According to the UNCTAD Global Cyberlaw Tracker, only 59% of countries have consumer protection laws, 71% have privacy laws, and 80% have developed cybercrime laws (United Nations Conference on Trade and Development [UNCTAD], 2021).

People and Organizations

In Ontario, another term for licensed CCPs is early years centres; these commercial businesses operate on a traditional organizational style with upper management and reporting lines flowing down from the top. Some organizations offer home child care as a branch of their business, and these operations follow the same organizational structure. Executive directors and managing directors facilitate the operational aspects of each department. Service System Managers in early childhood centres provide a high standard of quality programming and safety, build capacity to support clients, and ensure that licensed operations are compliant with legislative standards (OMSSA, 2020). Coordinators and administrators oversee their directives and guide the early childhood educators and assistants.

Problem Definition

The use of digital applications in education demonstrates a problem of consent and the need for training. The primary users of digital educational applications are parents and caregivers for daily collaboration, sharing content, and supplementing classroom learning using apps such as Google Classroom, HiMama, Storypark,

and Edmodo. Users are responsible for regulating and managing their privacy and information in their account settings and activity controls (Kudina & Verbeek, 2019). However, there needs to be clarity regarding where the responsibility lies in educational applications to ensure no third-party access.

While consent to share data is given upon accepting the terms and conditions, merely using the software can also indicate consent, which is problematic when the video subject is not of consenting age. Edmodo's terms of service state that educators who sign up for their service are presumed to represent and warrant legal authority from schools to provide consent (Common Sense, 2021).

Part of the problem lies in understanding the use of the collected data by the company that owns the app. After the information is collected, they have control of what happens with it, whether the data has been provided by the CCP or parent if they uploaded content. Storypark, an educational documentation software, positions the data as voluntarily provided personal information, but they control all aspects of the information. Data is stored for the contract's life, is shared with third parties for business development, and is used to track behaviour trends and assess their market position (Storypark, 2020). A recent report by Human Rights Watch (2022) indicates that educational apps are selling student information to third parties at a staggering rate, and this practice is largely unregulated.

In Canada, educators need the training to build digital privacy protection skills capacity. Educational Policy Institute Canada (2010) developed a framework for statistics on learning and education, which outlines that the early childhood education sector needs more research, training, and development at the provider level. Privacy and security training is recommended as one line of defence for information privacy, delivered through software providers or independently within the organization (IPCO, 2019; Student Privacy Compass, 2022). Training offers an understanding of sensitive data, retention and collection procedures, and policies governing continuous assessment practices in CCPs. In a study commissioned by the Office of the Privacy Commissioner of Canada, Hamel (2011) observed that "rights and protections do not exist online for safety and security, especially where privacy is concerned" (p.27).

Solutions

The authors believe educational/caregiving organizations should implement security measures to protect PII from external and internal data breaches. Adult-targeted digital literacy content is almost never presented with an educational focus; instead, it is only presented textually for reference. They communicate but do not sincerely attempt to teach. While graphical, interactive embellishments may not be necessary to keep an adult's interest, the methods usually used to teach youngsters could be used to communicate digital literacy principles—including privacy—more effectively (Hamel, 2011). Organizations must not only provide a choice for users to give their consent, but they have a duty of care to actively seek the consent of users by asking

multiple times and ensuring that informed consent is given (Robertson & Muirhead, 2022). CCPs can coordinate to take an active role in learning how to report education initiatives and performance for young children and how to keep large data sets confidential while collecting sensitive information.

The authors argue that teaching staff digital privacy requirements based on provisions of MFIPPA will help educators to practice digital privacy in the current surge and reliance on the internet for education. At present, educators need to be aware of the different legislation provided to enhance children's privacy and security when using digital learning applications. Equally, Canadian educators also require understanding of Canadian and American legislation for trans-border considerations and application. Policies should define the range of collected, stored and used information, and recommend consent forms from parents or designated early childhood educators before using students' information. The legislation will be ineffective in protecting against privacy risks without adequate staff training focused on understanding information security's meaning, significance, and scope within a learning environment.

Reflection on the Solutions

All stakeholders play essential roles in IT security strategies and decision-making for integrating digital platforms (Li et al., 2021). Data breaches result in fallout with severe consequences, including falling market value and high penalty costs (Shankar & Mohammed, 2020). However, organizations can recover from these fallouts through internal change processes (based on dynamic capabilities) to reclaim customers' confidence (Shankar & Mohammed, 2020). CCPs can initiate change for information privacy by assessing their organizational beliefs and values that inform technological adoption. Understanding technology's role in daily operations can help determine how valuable security measures are and what actions need to be taken by leaders. Without a clear policy for digital privacy in education, the message is "user beware."

Discussion Questions

1. How can organizations and parents collaborate to integrate a need for privacy when selecting educational apps that share private information?
2. Considering digital permanence, what might be shared online in 2022 that could impact that child when they are an adult?
3. What steps would you support in limiting the amount of information users share on learning platforms?
4. How can EdTech software providers protect PII and meet parents' efficient communication needs?
5. How might digital providers change the Terms of Service to be ethically accountable for explaining third-party access in plain language?
6. Within the digital platforms in Early Learning, what PII needs to be protected?

7. What needs to be done differently to improve privacy policy and digital safety for childcare providers?

Video

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/?p=302#oembed-1

Acknowledgement

The authors would like to thank Heather Leatham for their guidance and insight.

References

Bradshaw, S., Harris, K., & Zeifman, H. (2013, July 22). Big data, big responsibilities: Recommendations to the office of the privacy commissioner on Canadian privacy rights in a digital age. *CIGI Junior Fellows Policy Brief, 8*, 1-9. https://www.cigionline.org/publications/big-data-big-responsibilities-recommendations-office-privacy-commissioner-canadian

Cavoukian, A. (2011, January). *Privacy by design: The 7 foundational principles*. Information & Privacy Commissioner Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

Child Care and Early Years Act, S.O. 2014, c. 11, Sched. 1, 2014. https://www.ontario.ca/laws/statute/14c11?_ga=2.73153043.107555154.1655045667-1884507702.1655045667

Children's Online Privacy Protection Act, Pub. L. 105-277, div. C, title XIII, Oct. 21, 1998, 112 Stat.

2681-728 (15 U.S.C. 6501 et seq.) [1998]. https://uscode.house.gov/view.xhtml?path=&req=granuleid%3AUSC-prelim-title15-section6501&f=&fq=&num=0&hl=false&edition=prelim

Common Sense. (2021, August 26). *Privacy evaluation for Edmodo*. https://privacy.commonsense.org/evaluation/edmodo

Corcoran, B., & Wan, R. (2018, April 9). *China's NetDragon to acquire Edmodo for 137.5 million*. EdSurge. https://www.edsurge.com/news/2018-04-09-china-s-netdragon-to-acquire-edmodo-for-137-5-million

Educational Policy Institute Canada. (2010). *A framework for statistics on learning and education in Canada*. Council of Ministers of Education, Canada. http://www.cmec.ca/Publications/Lists/Publications/Attachments/257/cesc-data-framework-sept2010.pdf

European Parliament. (2016, April 27). *Regulations. Official Journal of the European Union, 59*, 119/1-119/31. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Durrani, R., & Alphonso, C. (2022, May 24). *Technology used by educators in abrupt switch to online school shared kids' personal information, investigation shows*. The Globe and Mail. https://www.theglobeandmail.com/canada/article-online-school-kids-privacy-data/

Federal Communications Commission. (2003, August). *Children's Internet Protection Act (CIPA)*, Pub. L 106–554, 2000. https://www.ntia.doc.gov/files/ntia/publications/cipareport08142003.pdf

Family Educational Rights and Privacy Act, Pub. L. 93-380, title V, Sec 513, Aug. 21, 1974,88 Stat. 571, [1974].

Flanigan, R. L. (2015, October 19). *Why K-12 data-privacy training needs to improve*. EducationWeek. https://www.edweek.org/technology/why-k-12-data-privacy-training-needs-to-improve/2015/10

House of Commons. (2019, June 21). *The Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Information and Privacy Commissioner of Ontario (IPCO). (2019). *Privacy and access to information in Ontario schools: A guide for educators*. https://www.ipc.on.ca/wp-content/uploads/2019/01/fs-edu-privacy_access-guide-for-educators.pdf

Hamel, van A. (2011). *The privacy piece: Report on privacy competencies in digital literacy programs in Canada, Britain, Australia, America, and Brazil*. MediaSmarts. https://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/The-Privacy-Piece.pdf

Human Rights Watch. (2022, May 25). *"How dare they peep into my private life?" children's rights violations by governments that endorsed online learning during the COVID-19 pandemic*. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Global Privacy Enforcement Network (GPEN). (2017, October). *GPEN sweep 2017: User controls over personal information*. UK Information Commissioner's Office. http://www.astrid-online.it/static/upload/2017/2017-gpen-sweep—international-report1.pdf

Herold, B. (2017, May 16). *Popular ed-tech platform Edmodo, hacked, faulted for ad-tracking*. Education Week. https://www.edweek.org/technology/popular-ed-tech-platform-edmodo-hacked-faulted-for-ad-tracking/2017/05

Klein, A. (2021, November 16). *EdTech usage is up. so are parent privacy concerns*. EducationWeek. https://www.edweek.org/technology/ed-tech-usage-is-up-so-are-parent-privacy-concerns/2021/11

Klose, M., Desai, V., Song, Y. & Gehringer, E. (2020). EDM and privacy: Ethics and legalities of data collection, usage, and storage. In A.N. Rafferty, J. Whitehill, V. Cavalli-Sforza, & C. Romero (Eds.), P*roceedings of The 13th International Conference on Educational Data Mining (EDM 2020)* (pp. 451-459). https://educationaldatamining.org/files/conferences/EDM2020/papers/paper_135.pdf

Leatham, H. (2017). *Digital privacy in the classroom: An analysis of the intent and realization of Ontario policy in context* (Masters dissertation, Ontario Tech University). https://hdl.handle.net/10155/816

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems, 38*(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Mollenkamp, D. (2022, August 16). *Popular K-12 tool Edmodo shuts down*. EdSurge. https://www.edsurge.com/news/2022-08-16-popular-k-12-tool-edmodo-shuts-down

Office of the Privacy Commissioner of Canada. (2020). *Appendix 3: Cross-border data flow and transfers for processing-jurisdictional analysis*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_app3/

Ontario Municipal Social Services Association. (2020, November). *Child care and early year services in Ontario*. https://www.omssa.com/docs/Child_Care_and_Early_Years_Services_in_Ontario.pdf

Poggi, N. (2021, February 4). *Three laws that protect students' online data and privacy*. PreyProject. https://preyproject.com/blog/en/three-laws-that-protect-students-online-data-and-privacy/

Robertson, L., & Muirhead, W. J. (2020). Digital privacy in the mainstream of education. *Journal of Systemics, Cybernetics and Informatics, 16*(2), 118-125. http://www.iiisci.org/journal/pdv/sci/pdfs/IP099LL20.pdf

Shankar, N., & Mohammed, Z. (2020). Surviving data breaches: A multiple case study analysis. *Journal of Comparative International Management, 23*(1), 35–54. https://doi.org/10.7202/1071508ar

Storypark. (2020, December 01). Privacy policy. https://main.storypark.com/privacy-policy

Student Privacy Compass. (2022). *Student privacy training for educators*. https://studentprivacycompass.org/resources/educatortraining/

United Nations Conference on Trade and Development [UNCTAD]. (2021, December 14). *Summary of adoption of e-commerce legislation worldwide*. https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

Vermont Agency of Education. (2022). *Edmodo resources for classroom teachers*. https://education.vermont.gov/edmodo/resources-classroom-teachers

Warren, S. D., & Brandeis, L. D. (1890). *The right to privacy*. Harvard Law Review, 4(5), 193-220. https://doi.org/1321160

Editors

Lorayne Robertson

Lorayne Robertson is an Associate Professor in the Faculty of Education at Ontario Tech University. She specializes in equity, leadership, policy and online pedagogy. She researches collaboratively on the student experience and instructor role in polysynchronous online environments with a particular focus on digital technologies and assistive technologies at the point of instruction in applied settings – both K-12 and higher education. Within the Faculty of Education, Lorayne has served as the Graduate Program Director, Assistant Dean, and BEd Director. Lorayne is a former Superintendent for a school district, an Education Officer for the Ontario Ministry of Education, a school principal and teacher. Currently, Lorayne is working on a SSHRC grant to investigate the experiences of persons who received Basic Income. She is also in a collaborative partnership with the Centre Franco Ontarien to research PD offered in virtual reality.

Bill Muirhead

Dr. Muirhead was the founding Associate Provost, Academic at the University of Ontario Institute of

Technology. As a founding academic administrator of the university, he was responsible for developing Canada's largest Technology Enriched Learning Environment, the Teaching and Learning Center, the Academic Success Center, the Health Education Technology Research Unit, the University Information and Technology Services and is currently a founding researcher of the EILAB in the Faculty of Education. Dr. Muirhead has overseen the development of university policies and governance structures pertaining to all aspects of the undergraduate curriculum and quality assurance. Dr. Muirhead's research interests included professional practices in online education; design of hybrid learning environments; policy support for developing and implementing learning object repositories; and the development and management of technological infrastructures in postsecondary institutions. An internationally recognized speaker, he has been the recipient of numerous awards for leadership and innovation in e-learning.

Authors

Lorayne Robertson

Lorayne Robertson is an Associate Professor in the Faculty of Education at Ontario Tech University. She specializes in equity, leadership, policy and online pedagogy. She researches collaboratively on the student experience and instructor role in polysynchronous online environments with a particular focus on digital technologies and assistive technologies at the point of instruction in applied settings – both K-12 and higher education. Within the Faculty of Education, Lorayne has served as the Graduate Program Director, Assistant Dean, and BEd Director. Lorayne is a former Superintendent for a school district, an Education Officer for the Ontario Ministry of Education, a school principal and teacher. Currently, Lorayne is working on a SSHRC grant to investigate the experiences of persons who received Basic Income. She is also in a collaborative partnership with the Centre Franco Ontarien to research PD offered in virtual reality.

Bill Muirhead

Dr. Muirhead was the founding Associate Provost, Academic at the University of Ontario Institute of Technology. As a founding academic administrator of the university, he was responsible for developing Canada's largest Technology Enriched Learning Environment, the Teaching and Learning Center, the Academic Success Center, the Health Education Technology Research Unit, the University Information and Technology Services and is currently a founding researcher of the EILAB in the Faculty of Education. Dr. Muirhead has overseen the development of university policies and governance structures pertaining to all aspects of the undergraduate curriculum and quality assurance. Dr. Muirhead's research interests included professional practices in online education; design of hybrid learning environments; policy support for developing and implementing learning object repositories; and the development and management of technological infrastructures in postsecondary institutions. An internationally recognized speaker, he has been the recipient of numerous awards for leadership and innovation in e-learning.

James Robertson

James Robertson is the Coordinator of the *Cyber Security Program* at Fanshawe College. In addition, he teaches and designs university courses in cybersecurity and policing. He is a former sworn Special Constable with 20 years of experience in security and law enforcement also working as an IT Security Systems Specialist and digital investigator. As a graduate of Ontario Tech U, his research publications and presentations explore the nexus of policing and digital technologies, especially cybercrime, digital forensics, and cybersecurity.

Laurie Corrigan

Laurie Corrigan is a Director of Education with the Catholic District School Board of Eastern Ontario. She has been a Superintendent in charge of Special Education, Equity and Technology and other areas. Her experience includes research in the area of safe schools legislation, digital privacy, cyberbullying, and restorative practices.

Heather Leatham

Heather has worked in education for over 20 years as both a classroom teacher, a digital literacy resource teacher, and is currently a secondary school vice-principal. She holds degrees from the University of Ottawa, Western University, York University and a Masters of Art in Educational and Digital Technologies from the University of Ontario Institute of Technology. Her academic interests are in digital privacy and technology use in the classroom.

Dr. Robertson and Dr. Muirhead (Eds) would like to acknowledge the support of e-Campus Ontario for funding to support the *Digital Privacy: Leadership and Policy* graduate course and e-book.

We also acknowledge the stellar work of Chris D. Craig and Amel Belmahdi, graduate research assistants in the Master's of Education and Digital Technology program at Ontario Tech U for sharing their expertise in support of the authors.

It is the diligence and commitment of this collaborative team that made this e-book possible.