TROUBLING CLOUDS

Gaps affecting privacy protection in British Columbia's K-12 education system.

MATTHEW A. J. LEVINE

FIPA BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

We would like to thank several contributions that made this work possible.

Former Executive Director Sara Neuert, through stakeholder consultation, played a key role in initiating this project.

We thank the numerous parents, educators, and students who contacted us over the years to ask questions and raise concerns about privacy in BC's education system. Particular thanks is owed to the participants in the two public forums that were held as part of the research process for this report.

Significant consultations included the British Columbia Teachers Federation. BCTF works to engage members and increase education resources. To deliver quality education in a resilient system requires constant consideration of the gaps that impact students, teachers, parents, and administrators. This report highlights gaps in areas of privacy.

None of this would have been possible without the support and commitment to the programs and projects that intersect privacy and transparency from the British Columbia Law Foundation.

THE LAW FOUNDATION OF BRITISH COLUMBIA

Troubling clouds: Gaps affecting privacy protection in British Columbia's K-12 education system.

Matthew A. J. Levine for the British Columbia Freedom of Information and Privacy Association

ISBN 978-1-7772225-1-2

Troubling clouds: Gaps affecting privacy protection in British Columbia's K-12 education system by Matthew A. J. Levine for the British Columbia Freedom of Information and Privacy Association is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. Based on a work at https://fipa.bc.ca/.

Designed by Nelson Agustin

EXECUTIVE OVERVIEW

Our K-12 public education is heading to the cloud.

Software that was once procured by school boards and contained within specific devices has moved to the cloud. Research for this report revealed that one cloud-based internet platform, and the software applications that it makes available to school boards, teachers, and students, is being used in every region of British Columbia. That platform is marketed by Google and called G Suite for Education.

Certainly, Silicon Valley's internet start-ups and funds are united in seeking new ways to move computing services from the mainframe to the cloud, and to move software from the desktop to the browser. The education sector is an attractive market for these trans-national companies. As one Silicon Valley billionaire wrote in the pages of the *Wall Street Journal* "software is eating the world".[1]

The provincial government has appeared to welcome this trend, writing in the Province's Education Plan for the "smart use of technology in schools" to help students "thrive in an increasingly digital world." [2] This is certainly a laudable ambition. There is no question that cloud-based software applications targeted at the education sector can facilitate the use of new technologies, from private digital devices to the internet itself. They also facilitate a broader shift from paper-based to screen-based instruction as both student outputs and teacher evaluation can be digitized.

But what is the cost to student privacy now and into the future?

Canadian law recognizes that the limits of personal privacy very often define the limits of our freedom. The Supreme Court of Canada has, for instance, stated that: "it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free society."[3] Therefore, the

---

[1] Marc Andreessen, "Why Software is Eating the World" (Aug 20, 2011) Wall Street Journal C2 <https://www.wsj.com/articles/SB10001424053111903480904576512250915629460>.

[2] British Columbia, Ministry of Education, *BC's Education Plan* (Victoria: 2011), at 7 <http://www.llbc.leg.bc.ca/public/pubdocs/bcdocs2011_2/508308/bc_edu_plan.pdf>.

[3] R. v. Duarte, [1990] 1 SCR 30.

intimate connection between personal information and personal liberty is at the core of information privacy. This connection may be said to be even more sacrosanct where the personal information belongs to children and is, thus, by its very nature, sensitive.

In British Columbia, the *Freedom of Information and Protection of Privacy Act* ("FOIPPA")[4] governs the public sector. FOIPPA establishes quasi-constitutional rights concerning personal information. Under FOIPPA, students in British Columbia's public schools have rights regarding the collection, use, or disclosure of their personal information. Simultaneously, under FOIPPA, British Columbia public bodies have obligations to take reasonable measures to protect the security of personal information and thereby safeguard those privacy rights. These obligations are not vitiated merely because a public body elects to engage an external service provider.

Privacy concerns associated with contracting out are not new. It has been more than a decade since the Information and Privacy Commissioner for British Columbia's ("Privacy Commissioner") landmark report on managing privacy risks associated with contracting out was released.[5] The Privacy Commissioner included twenty specific recommendations that were subsequently accepted in full by the provincial government. The use of software applications accessed through internet platforms, however, may be a sufficiently novel form of contracting out that it has raised unanticipated challenges for the public sector. Why? Because, simply put, internet platforms today have amassed so much market power that they are credibly able to insist on a set of 'take it or leave it' terms of use, rather than negotiating a service agreement.

Today, in early 2020, the COVID-19 emergency has necessitated the closure of schools and the province has temporarily loosened privacy safeguards for use of platforms and applications.[6] COVID-19 has, perhaps, had the unintended

[4] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, *c. 165.*
[5] Information & Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (October 2004), online: *<https://www.oipc.bc.ca/special-reports/1271>*.
[6] *Ministerial Order No. M085* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085>; *Ministerial Order No. M180* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m180>

consequence of drawing attention to the use of platforms and applications in the public education system. This report concludes that we, as a society, cannot ignore the related privacy concerns any longer.

Software applications and internet platforms are almost certainly going to be part of British Columbia's classrooms for the foreseeable future. Alongside the advantages associated with introducing students to the internet, increasing the use of software applications in the classroom also opens the door to privacy risks. Now is the time for all concerned stakeholders to think seriously about systematic solutions for managing these risks.

RECOMMENDATIONS:

1. The Ministry of Education should play a more active role in supporting the procurement of cloud computing services. The Ministry's strategic role in the public education system and relatively sophisticated information technology capacity should be leveraged to maximize resources, exchange knowledge, and develop best practices for privacy risk management.
2. Privacy Commissioner should make use of the International Conference of Data Protection and Privacy Commissioners' ("ICDPPC") activities regarding online platforms in public schools. Specifically,
    a. Actively participate in the ICDPPC Digital Education Working Group's activities, including the questionnaire that was circulated by the French data protection authority and Canada's OPC in June 2019, so as to exchange best practices with other jurisdictions;
    b. In light of commitments and norms embodied in ICDPPC *Resolution*, formulate a guidance document for public bodies in the education sector so that they may fully comply with their privacy obligations when engaged in contracting out cloud computing services.
3. School boards should ensure they have information technology and privacy expertise necessary to:
    a. Conduct substantive privacy impact assessments on private sector providers of information technology services;

   b. Develop policies and procedures to assess, approve, and support the use of internet platforms and software applications without compromising students' privacy rights or shifting the privacy risk management burden;
   c. Provide training and support for teachers in respect of classroom technology and privacy;
   d. As required and appropriate, seek valid, informed and meaningful consent from individuals, i.e. students and guardians.
4. Ministry of Education and school boards should strengthen co-ordination to:
   a. Negotiate, as necessary, service agreements with service providers who may be unwilling to negotiate with individual school districts;
   b. Establish a shared mechanism for rating and otherwise exchanging knowledge about internet platforms and software applications;
   c. Maintain said mechanism while taking on-board feedback from students, guardians, and teachers.

TABLE OF CONTENTS

1. INTRODUCTION

If you step into a typical British Columbian school, you will find students making extensive use of an increasingly wide range of information technologies. In particular, multinational corporations headquartered in the United States, such as Google and Microsoft, now routinely provide their office software to BC school districts without charge as part of broader marketing campaigns aimed at the education sector. These proprietary internet platforms offer education authorities a seemingly free mechanism for contracting out general information technology services and specific software applications. The contracting out of software applications on the one hand and data storage on the other hand through cloud computing services is an important and growing trend.

The increasing use of and reliance on software applications as a natural part of providing public education is contemplated, obliquely, by the Province's Education Plan that now calls for the "smart use of technology in schools" to help students "thrive in an increasingly digital world."[7] This is certainly a laudable ambition. However, there are concerns that local school boards are poorly positioned and inadequately resourced when it comes to evaluating "internet platforms" and "learning management systems" marketed by giant American companies, such as Google. Both terms will be discussed in this report.

The research and consultations undertaken for this report make it clear that one obstacle to evaluating the services marketed by Google, Microsoft and others is that lay people do not always know exactly what is involved in the 'Software as a Service' business model associated with cloud computing. Some preliminary points of orientation are provided by two leading scholars of information technology and the law. Jonathan Zittrain, Professor at Harvard Law School, has argued for more than a decade that "the best physical representation of the genius of the Internet … is found in an hourglass."[8] In an influential article from 2006, Zittrain wrote that "the Internet's framers intended an hourglass design,

[7] British Columbia, Ministry of Education, *BC's Education Plan* (Victoria: Ministry of Education, 2011) at 7 <http://www.llbc.leg.bc.ca/public/pubdocs/bcdocs2011_2/508308/bc_edu_plan.pdf>.

[8] Jonathan Zittrain, "Chapter 45 – Internet" in Claudy Op den Kamp and Dan Hunter, eds, *A History of Intellectual Property in 50 Objects* (Cambridge: Cambridge University Press, 2019) 369 at 369, online: <https://ssrn.com/abstract=3373352>

with a simple set of narrow and slow-changing protocols in the middle, resting on an open stable of physical carriers at the bottom and any number of applications written by third parties on the top."[9] According to the hourglass metaphor, the broad bottom of the internet is made up of terrestrial infrastructure, i.e. cable and fibre, that transmits data packages. Meanwhile, the broad top of the internet are the software applications that codify "what we might do when we can exchange data with one another, whether email, web browsing, or videoconferencing."[10] This is, in turn, consistent with the displacement of software from specific, user-owned machines to instead being hosted in the digital cloud: a 'cloud' is, naturally enough, above the 'top' of any earth-bound structure. The notion of cloud computing is examined further in section 2.

While Zittrain's hourglass metaphor has been influential – especially in debates about net neutrality – and helps readers to visualize an otherwise highly abstract technology, he perhaps does not devote enough attention to the sand that moves back and forth from the physical infrastructure at the bottom to the software applications at the top. What is this sand, exactly? A powerful answer to that question is provided by the University of Toronto Law Professor Ariel Katz. Katz argues that:

> Data is said to be the essential capital stock of the data-driven economy, built around massive data collection and various business models for profitably sharing and using it. Metaphors such as "the new oil" or "the new gold" reflect this value extraction potential for businesses and they conjure up the "wants to be expensive" theme. These metaphors emphasize the money that can be made by those who control data — the private benefits that they might derive from its exploitation, not the aggregate value shared by society. [11]

[9] Jonathan Zittrain, "The Generative Internet" (2006) 119:7 Harv L Rev 1974 at 1988. <www.jstor.org/stable/4093608>.

[10] Jonathan Zittrain, "Chapter 45 – Internet"

[11] Ariel Katz, "Data Libera? Canada's Data Strategy and the Law of the Sea", online: (May 2018), Centre for International Governance Innovation <https://www.cigionline.org/articles/data-libera-canadas-data-strategy-and-law-sea>.

In a word, the sand of the internet is data.[12] Furthermore, it is data created by individual users and by extension, in many cases, information about those individuals. The extent to which user-generated information is personal information raises complicated legal issues that will be addressed in later sections of this report. Here, at the outset, it is sufficient to note that, as reviewed by Katz, this data is clearly valuable enough that sophisticated business models and massive private fortunes have been built around its extraction and privatization. The ethical, policy, and legal issues associated with this development in public school classrooms are examined in this report.

The report begins by introducing the methodology. Section 2 reviews the factual landscape, followed by section 3, which introduces the legal framework for privacy and the public education system in British Columbia. Section 4 examines privacy rights and privacy risks under British Columbia law in light of the facts known about the use of software applications in today's classrooms. Section 5 reviews the principles and best practices that are emerging from other jurisdictions and transnational networks regarding the use of private, cloud-based software applications in public school classrooms. Section 6 concludes the report with final recommendations.

1.1 Research Methodology

There are no province-wide statistics regarding the use of software generally or cloud-based software applications specifically in British Columbian schools. For the purpose of preparing this report, we have undertaken qualitative and quantitative open source research, prepared the relevant freedom of information requests under the *Freedom of Information and Protection and Privacy Act* ("FoI Requests"), and conducted multiple public consultation sessions.

The qualitative and quantitative research conducted for this report has reviewed a variety of publicly available sources of information. One part of this research process was a review of academic materials prepared within British Columbia,

[12] An early theorization of this phenomenon can be found in the work of the American management guru Peter Drucker who proposed that a "knowledge based economy" is predicated on the monetization of data and information. Peter Drucker, The Age of Discontinuity (New York: Harper & Row, 1969).

Alberta, and Ontario education faculties. Relevant scholarship includes writing and analysis, both published and unpublished (i.e. approved graduate dissertations). It touches on themes of information technology management within Western Canadian school boards, the pedagogical advantages, and the limitations of information technology-based lesson plans.

A second part of the open source research process involved reviewing media information relating to the education technology industry. This included mainstream news channels such as the Canadian Broadcasting Company ("CBC") in Canada. It also included industry-focused blogs created by educators, trainers, salespeople, and etcetera. It further included research and analysis of reports created by think tanks and advocacy organizations.

The second aspect of the overall research methodology was to prepare FoI Requests that were sent to school boards, asking for information about the use of software applications in the specific, geographic-district administered by the relevant school board. The requests were not specific to any particular software application.

The third aspect of the overall research methodology was to conduct public consultations. These sessions were, for logistical reasons, only conducted in the Lower Mainland of the Province. The sites were in Surrey and in Richmond. Although we were not able to travel outside the Lower Mainland for these public consultations, we did hear from interested members of the public located in other parts of the province. Furthermore, at the public consultation sessions, we were able to engage with a diverse cross section of stakeholders including parents, teachers, and education technology specialists.

In addition to the above, research was conducted on the specific usage of Google's G Suite for Education in British Columbia.[13] We reviewed both documentary and anecdotal information that provides considerable evidence of

[13] Craig Desson, "As Google for Education Tools Enter Classrooms Across Canada, Some Parents are Asking to Opt-out" online: (June 11, 2018), CBC Radio <https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935/as-google-for-education-tools-enter-classrooms-across-canada-some-parents-are-asking-to-opt-out-1.4694939>. Accessed 7-5-20. According to Desson: "Statistics are hard to come by, but the Alberta Ministry of Education told Spark that about 90 per cent of public school authorities are using G Suite for Education to some extent. It's being used in every public school in Nova Scotia as well."

how Google's services are being used today in British Columbian schools. Documentary resources obtained and reviewed for this report include Privacy Impact Assessments (PIAs) prepared at the school district level; letters to guardians, i.e. requesting consent for use of Google's G Suite for Education, prepared by both school districts and individual schools; public-facing websites maintained by schools or school districts that describe the use of G Suite for Education in the classroom.

As above, there are no province-wide statistics regarding the use of Google's G Suite for Education software applications in British Columbia. However, based on the research conducted for this report we can say that school districts, in all parts of the province, intend to or already have created G Suite for Education accounts. Table 1 lists specific districts that were identified in our research.

Table 1: School Districts Identified as Using Google's G Suite for Education

Region	School District(s) using Google
The Islands	Greater Victoria,[14] Saanich,[15] Qualicum, and Nanaimo Ladysmith[16]
Lower Mainland	West Vancouver,[17] Sea to Sky,[18] and New Westminster[19]

[14] Greater Victoria School District, *Privacy Impact Assessment for School District No. 61 (Greater Victoria) and School District No. 63 (Saanich)* (2018), online: <https://www.sd61.bc.ca/wp-content/uploads/sites/91/2018/09/GSuite-PIA-SD61_63.pdf>.
[15] Greater Victoria School District, *Privacy Impact Assessment for School District No. 61 (Greater Victoria) and School District No. 63 (Saanich)* (2018), online: <https://www.sd61.bc.ca/wp-content/uploads/sites/91/2018/09/GSuite-PIA-SD61_63.pdf>.
[16] Nanaimo Ladysmith School District, *Privacy Impact Assessment for School District No. 68*, online: <https://www.sd68.bc.ca/wp-content/uploads/GSFE_PIA_NLPS.pdf>.
[17] West Vancouver School District, "Information Letter & Permission Form" (2015), online: Computer Using Educators of British Columbia <*https://cuebc.ca/resources/google-apps-for-education*>.
[18] Sea to Sky School District No. 48, "Board Meeting no.924" (September 2018), online: <https://sd48seatosky.org/wp-content/uploads/2018/09/18-09-12-BM-O-Agenda-PACKAGE.pdf>.
[19] New Westminster School District, "Queensborough Middle School, School Calendar" (2019), online: <https://queensboroughschool.ca/parents/notices-information/school-calendar

Thompson Okanagan	Central Okanagan (SD 23)[20]
BC Rockies	Kootenay-Columbia (SD 20) [21]
Central BC	Kamloops (SD 73)[22]
Northern BC	Campbell River[23]

2. INFORMATION TECHNOLOGY IN BRITISH COLUMBIA'S CLASSROOMS

In British Columbia's K-12 public education system, information technology sponsorship by large, multinational corporations is not uncommon. Companies head-quartered in the United States, such as Dell, IBM, and Apple, have traditionally given computer hardware to British Columbian schools as a means of cultivating future customers. As part of a broader marketing campaign aimed at the education sector, Google and Microsoft have started to gift software applications to school districts for free, thereby creating a significant shift in today's classrooms from hardware to software. This report explores the increasing number of schools which are making greater use of software applications for everything from document sharing to multimedia presentations and student evaluations. Indeed, the Province's Education Plan now calls for the "smart use of technology in schools" to help students "thrive in an increasingly digital world."[24]

---

[20] Central Okanagan School District 23, "Quigley Elementary, Google Classroom Inquiry" (2020), online: <http://www.qge.sd23.bc.ca/clp/our%20inquiry%20process/googleclassroom/default.aspx#/>.

[21] School District 20 - Kootenay-Columbia, "Privacy Agreement", online: <https://www.sd20.bc.ca/gsuitestaff/>.

[22] School District No. 73 Kamloops/Thompson "Acceptable Use Guidelines", online: Google Apps for Education, <https://sites.google.com/a/gedu.sd73.bc.ca/sd73gafe/privacy/acceptable-use-guidelines>.

[23] School District 72 - Campbell River, *Privacy Impact Assessment for Google Suite for Education (GSFE)*, online: <https://www.sd72.bc.ca/studentsparents/GSFE/Documents/GSFE%20PIA%20%20for%20SD72%20FINAL%20DRAFT.pdf>>.

[24] *BC's Education Plan* (Victoria: Ministry of Education, 2011) at 7 <http://www.llbc.leg.bc.ca/public/pubdocs/bcdocs2011_2/508308/bc_edu_plan.pdf>.

The increasingly intimate relationship between public education and information technology, especially software applications, is visible not just in British Columbia but across North America and indeed the world. For example, the Education Technology Industry Network ("ETIN") (an industry-backed advocacy and research group in the United States), values the market for selling software to educational institutions at more than $8 billion USD annually, and growing at 5% each year.[25] An independent analysis of the education technology market's prospects during the period 2018–2024 predicts annual expansion at 15.4%.[26] Indeed, Marc Andreeson, founder of Netscape, which at one time was viewed as a competitor to Google, famously quipped in the Wall Street Journal that, "software is eating the world."[27]

Corporate donations may well have existed for longer than Silicon Valley. The decision by Google, Microsoft and other tech giants to actively market free software to public schools, however, goes well beyond charity. Various explanations can and have been advanced as to why a multinational corporation would distribute its product with no up-front charge.[28] One explanation is that, in doing so, schools will continue to use the software even after their free trials end, thereby locking themselves into contracting educational services to private service providers.[29] More pertinently, and as examined throughout this report, the

---

[25] John Richards & Leslie Stebbins, *2014 US Educational Technology Industry Market: PreK-12* (2014), online webinar: SIIA US Ed Tech Market Surveys < https://www.siia.net/Divisions/ETIN-Education-Technology-Industry-Network/Resources/Webinar-Library/2014-US-Education-Technology-Market-PreK-12-Report >. ETIN is an extension of the Software & Information Industry Association. It divides the PreK-12 education technology market into two categories: hardware and non-hardware. The 2014 report values the overall PreK - 12 non-hardware education technology market at $8.38 billion, compared to the previous year's valuation of $7.9 billion.

[26] Global Education Technology Market, *Global Education Technology Market: Drivers, Restraints, Opportunities, Trends, and Forecast up to 2024* (November 2018), online: <https://www.researchandmarkets.com/research/pq8kbz/global_education?w=4>.

[27] Andreessen, "Why Software is Eating the World"

[28] For a relatively halcyon take, readers may wish to consider the writing of WIRED magazine editor Chris Anderson: Chris Anderson, *Free: The Future of a Radical Price* (Random House, 2009). A less enthusiastic perspective is provided by Columbia University law professor: Tim Wu, *The Attention Merchants: The Epic Scramble to get Inside our Heads* (Toronto: Random House, 2016)).

[29] Lisa Austin, et al *Seeing Through The Cloud*, at 21, online: University of Toronto (2015) <https://www.ryerson.ca/content/dam/politics/docs/internal/SeeingThroughTheCloud-BohakerAustinClementPerrin-150915.pdf>.

use of internet-based software applications is a form of contracting out, where an inherently public function (i.e. K-12 education) is being delegated to private service providers. By making use of commercial software applications and the cloud computing capacity that the applications run on, British Columbian school districts are engaged in contracting out.

In recent decades, Canadian governments have used the contracting out model to reduce costs and increase flexibility. This model has been an important means of satisfying calls for balanced budgets and reduced taxes.[30] Schools, especially post-secondary institutions, have contracted out educational services to make use of the economies of scale that extra-national platforms such as Google and Microsoft offer.[31] Contracting out of public services may, however, also lead to concerns that related decisions lack sufficient transparency and that public bodies, unlike corporations, should not make decisions based solely on economic factors. Furthermore, a recent report on contracting out in Canada's higher education sector co-authored by a University of Toronto Law professor, Lisa Austin, has found that Google's and Microsoft's standard terms do not specify which privacy laws they follow in storing customer data.[32] For current purposes, it is not necessary to weigh too deeply into broader debates about contracting out in British Columbia or assess outsourcing writ large. It is sufficient to recognize that public services are being provided by private firms, and therefore the relationship between the government and the software companies is, broadly speaking, parallel to the specific relationship that is created under a service contract. This report explores the ethical, policy, and legal implications where there are no such service contracts, with an emphasis on concerns and risks for students' privacy.

Google provides a particularly useful example for understanding the increased role of software applications in British Columbia's classrooms. Indeed, Google's

---

[30] Penny Gurstein and Stuart Murray, *From Public Servants to Corporate Employees: The BC Government's Alternative Service Delivery Plan in Practice* (Vancouver: Canadian Centre for Policy Alternatives, October 2017) <https://www.policyalternatives.ca/sites/default/files/uploads/publications/BC_Office_Pubs/bc_2007/bc_FromPublicServants.pdf>. Also, Office of the Privacy Commissioner of Canada, *Privacy and Outsourcing for Federal Institutions*, online: (January 2014) <https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/outsourcing/02_05_d_57_os_02/>.

[31] Austin et al, *Seeing Through The Cloud*,at 16

[32] Austin et al, *Seeing Through The Cloud*,at 15

education-sector targeted offering, i.e. G Suite for Education, is used as a case study in parts of this report. We have found three particularly pressing concerns: (1) the lack of privacy training for teachers; (2) the absence of risk-mitigation by relevant public bodies; and (3) an over-reliance on parent / guardian consent forms.

The remainder of this section reviews specific factual issues related to software applications generally and Google's education-focused platform for providing software applications in particular. The section addresses the following questions:

1. How does a technical overview of cloud computing help elucidate key terms used in this report such as "internet platform", "software applications", and "learning management system"?
2. What are the most commonly used examples of these technologies, especially internet platforms, in British Columbia's schools?
3. Which BC school districts are presently using Google's internet platform; and, how is this technology being used?
4. What training materials have been prepared by Google, school boards, and the province?

2.1 Cloud Computing: Internet Platforms, Software Applications, and Learning Management Systems

As software usage becomes a significant - and in some cases unavoidable - feature of public education in British Columbia, questions naturally arise about the underlying technology. Information technology terminology is, by its very nature, abstract. Indeed, through the consultations for this report it became clear that abstract terminology can become an impediment to shared meaning and genuine communication. It is also correct that a lot of the fashionable jargon surrounding information technology has been created for marketing purposes. Take for example the notion of an "E-learning platform". The International Conference of Data Protection and Privacy Commissioners ("ICDPPC") – whose recent initiative we review in in Section 5 – defines the term "E-learning platform" very, very broadly whereby

> E-learning platforms refer to the online technological tools and media that assist in the communication of knowledge, its development and the interaction among educators, students and educational institutions. E-learning platforms typically involve a variety of devices (such as computers, tablets and mobile devices), data processing and usage models (in classroom, online courses) and actors (students, educators, educational institutions, platform providers, application providers).
>
> The term excludes pure school management tasks operated on back office applications implemented by education authorities such as transfer and assignment of educators or administrative management of students at school that are not related to learning.[33]

This definition is clearly very broad. For example, it refers to "online technological tools and media that assist in the communication of knowledge, its development and the interaction among educators, students and educational institutions." Under this definition, it would not be unreasonable to conclude that a video-sharing website such as YouTube is included so long as it is used by teachers, students, and schools. For that matter, there is no obvious reason why the definition could not also capture an online bulletin board that facilitates file sharing, such as BitTorrent.

There may be reasons for the ICDPPC to have cast a broad net; however, the consultations for this project have made it clear that the use of a catch all term results in confusion. The ambiguity and uncertainty that results from calling any type of information technology used in a school an "E-learning platform" is a potential obstacle to public debate. We aim to mitigate this obstacle through the current background section. Our goal is to disentangle "internet platform", "software application", and "learning management system" as three distinct

[33] 40th International Conference of Data Protection and Privacy Commissioners, "Resolution on E-Learning Platforms" (Brussels, 23 October, 2018) at 2 online: <http://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf>.

pieces of information technology. We do this by situating the above terms in a general overview of cloud computing.

Cloud computing is a relatively new form of information technology infrastructure. It has, however, been considered by both the federal Office of the Privacy Commissioner ("OPC")[34] and the Information and Privacy Commissioner of Ontario ("IPC").[35] While the OPC examined cloud computing from the perspective of consumers, the IPC considered it from the perspective of organizations. As reviewed below, these two perspectives are ultimately complimentary.

The OPC addressed the nature of cloud computing in a 2010 public report titled *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing* ("*Reaching for the Cloud(s)*"). In *Reaching for the Cloud(s)*, the OPC found that cloud computing means that a software application is stored on the internet, and accessed via any device.[36] It further wrote that, for the purposes of that software application, the user's device becomes a 'dumb terminal', a machine that interacts with a cloud-mainframe in order to store, retrieve, or manipulate data."[37] This perspective emphasizes the fact that cloud computing removes software from the user's device and induces the user to instead access the software through an internet connection. The OPC's description of cloud computing focused on the perspective of consumers and users; however, there are actually two types of users who are provided with software applications through cloud computing infrastructure: intermediary-users and end-users.

A complementary perspective on cloud computing has been articulated by the IPC. In *Thinking About Clouds? Privacy, Security and Compliance Considerations for Ontario Public Sector Institutions* ("*Thinking about Clouds*"), the IPC addresses

---

[34] Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing* (March 2010) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/cc_201003/>.

[35] Information and Privacy Commissioner of Ontario, *Thinking About Clouds? Privacy, Security and Compliance Considerations for Ontario Public Sector Institutions* (February 2016) online: < https://www.ipc.on.ca/wp-content/uploads/2016/08/thinking-about-clouds-1.pdf>.

[36] Austin et al, *Reaching for the Cloud(s),* 3, 13.

[37] Austin et al, *Reaching for the Cloud(s),* at 2

the computing capacity advantages of cloud computing. From this perspective, cloud computing is first and foremost a means to provide information technology infrastructure as a service. That is, rather than investing in its own computing infrastructure, an organization can make use of equivalent or superior computing resources that are owned by a service provider. To note, the organization must have access to sufficient internet connectivity.[38] The IPC in turn notes that public sector organizations are increasingly using cloud computing services,[39] and that this includes the Software as a Service ("SaaS") model,[40] which is utilized by Google's G Suite for Education. In the SaaS model, a cloud provider licenses the use of on-demand software applications to customers, both end-users, i.e. employe, and intermediary-users, i.e. the employer.[41] Software applications commonly made available through the SaaS model include office productivity, online collaboration, and data management.[42] An office productivity app that is commonly used by end-users through a SaaS model is Google's G Mail, while an office productivity app that is commonly licensed by intermediary-users for use by its staff is Microsoft's Office 365, which includes a webmail software application as well as document processing and database. The IPC notes that SaaS providers typically host the applications on their own infrastructure and thus make use of what is known as a private cloud.[43] This private cloud model is used by both Google and Microsoft.[44] In principle, there are a large number of ways that customers, whether end-users or intermediary-users, can be billed for the services provided by a SaaS provider: by the number of end-users, the time of use, the network bandwidth consumed, the amount of data stored or the duration of stored data. Finally, in a SaaS model, the intermediary-user has no control over

[38] Information and Privacy Commissioner of Ontario, *Thinking about Clouds*, at 1.
[39] Information and Privacy Commissioner of Ontario, *Thinking about Clouds,* at 1.
[40] Information and Privacy Commissioner of Ontario,*Thinking about Clouds*, at 3-4 . It also notes that cloud services are offered to the market through three primary models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).
[41] Information and Privacy Commissioner of Ontario, *Thinking about Clouds,* at 4 .
[42] Information and Privacy Commissioner of Ontario, *Thinking about Clouds,* at 4.
[43] Information and Privacy Commissioner of Ontario, *Thinking about Clouds,* at 2.
[44] Cloud infrastructure is typically marketed through one of four business models –i.e. public, private, community and hybrid – with so-called "public clouds" and "private clouds" being particularly relevant for current purposes. These terms do not refer to the private sector vs public sector distinction with which some readers may be most familiar. A prominent example of a public cloud is Amazon Web Services, which Public clouds refer to cloud computing services that are owned and managed by one provider for multiple organizations that pay to use the service.

the cloud infrastructure and only limited capabilities to configure software applications.[45]

Canadian privacy and data protection authorities have, therefore, considered cloud computing from, at least, two perspectives: end-users (i.e. consumers of software applications) and intermediary-users (i.e. organizations that rely on cloud services in order to forego investment in computing capacity). In the current case, as explored further in the following sections, British Columbia school boards are intermediary-users of Google's G Suite for Education.

In turn, in the same way that Facebook is an "internet platform" because its users gain access to a suite of software applications, G Suite for Education is an "internet platform" because its users also gain access to a suite of software applications. The terminology of internet platforms, therefore, has at least two connotations: it refers to a business that makes a service available through a webpage, and it refers to the suite of apps that constitute the specific service that is being made available.[46] The relevant difference between Facebook and G Suite for Education is that Facebook's users are individuals who enter into an end-user agreement with Facebook whereas G Suite for Education's users are organizations, such as school districts. Having entered into an intermediary-user agreement with Google, these organizations then create profiles for their staff and students. As a result, staff and students do not directly contract with the information technology service provider of the software applications and internet platforms being used in British Columbian public schools.

As noted above, when G Suite for Education was first brought to market, Google negotiated intermediary-user agreements with each of its partners, which were typically universities. At the current point in time, the contractual relationship for this service, however, is not negotiated. Rather, Google has made a standing offer in the form of its terms of use for G Suite for Education. The acceptance of these

---

[45]Information and Privacy Commissioner of Ontario, *Thinking about Clouds, at 4* .

[46] In short, the basic 'deal' of platforms, such as Google, is this: in exchange for access to the software on the platform, users supply their data into that same platform. In the case of an Ed Tech Platform, it is not the apps that change, but rather the type of user as users of an Ed Tech Platform are by definition enrolled in an education institution.

terms of use by a given school district creates a contractual relationship akin to an intermediary-user agreement.

Furthermore, G Suite for Education is not only a platform, it is also the brand name given to a suite of software applications made available by Google, as a service, to its users. As examined in more depth below, the majority of the software applications made available through G Suite for Education are simply re-branded versions of Google's commercial internet ecosystem. Nevertheless, the G Suite for Education suite of software applications does contain one specific piece of software that is specific to education, which is called Google Classroom. Google Classroom, in turn, contains online collaboration and data management functionalities. It is, in short, an example of what is often referred to within the education technology industry as a learning management system. The distinction between internet platform and learning management system becomes clearer by looking at specific examples as used in the province's public education system today. This is the subject of the next subsection.

2.2 Internet Platforms in British Columbia Schools

According to research conducted for this report, the most frequently used internet platforms in British Columbian schools comprise two major categories: platforms operated by the public sector, especially the provincial government; and platforms marketed by the private sector.

2.2.a Public Platforms

As a preliminary matter, it is instructive to note the Ministry of Education's back-office system for managing student information is premised upon assigning a Personal Education Number ("PEN") to students entering the public education system.[47] PEN was first introduced in the 1980s and has been widely used by both K-12 and post-secondary institutions since the 1990s. It is a unique nine-digit identification code that follows each student's movement through the public education system. For example, students are expected to use their PEN when

[47] Official Website of the Government of British Columbia, Education and Training "Personal Education Number (PEN)" online: <https://www2.gov.bc.ca/gov/content/education-training/k-12/support/transcripts-and-certificates/studenttranscripts-services-help/personal-education-number>.

accessing provincial exam results or ordering secondary school transcripts.[48] While students may use their PEN to request that the public sector retrieve and share information, they may not use a PEN to directly access either the information itself or the system that manages that information.[49]

A variety of public-sector internet platforms are used in the system depending on practice in different parts of the province. For instance, in 2018, the Vancouver School Board indicated that student information may be stored in any of the following three platforms: MyEducationBC; CIMS; and/or DRUMS.[50] MyEducationBC, which is also referred to as MyEdBC, is a limited functionality platform that primarily provides student information system ("SIS") software. In turn, the SIS software enables students to access some information associated with their PEN. Although less information is available about CIMS and DRUMS, the platforms appear to be alternatives to MyEdBC as they serve a similar purpose, but they are provided by a different software company. MyEdBC is the most commonly used public platform with an 88% penetration rate across the province.[51]

2.2.b Private Platforms

Although the public sector provides a platform for accessing a very basic set of software applications, internet platforms and associated software applications provided by private, for-profit businesses play a much larger role.

---

[48] <https://www2.gov.bc.ca/gov/content/education-training/k-12/support/transcripts-and-certificates/studenttranscripts-services-help/personal-education-number>.

[49] <https://www2.gov.bc.ca/gov/content/education-training/k-12/support/transcripts-and-certificates/studenttranscripts-services-help/personal-education-number>.

[50] British Columbia Ministry of Education, *B. C. Graduation Program Handbook of Procedures* online: (July 2019) at 7 <https://www2.gov.bc.ca/assets/gov/education/administration/kindergarten-to-grade-12/graduation/handbook_of_procedures.pdf >.

[51] Peter Holowka, "IT Leadership and Cloud Computing Adoption in Western Canadian K-12 School Districts" (University of Calgary: Unpublished doctoral thesis, 2018) online: <https://prism.ucalgary.ca/handle/1880/107467> MyEdBC and the associated SIS software, i.e. BCeSIS, are managed by the province's Ministry of Education.

2.2.b.i Google

The private-sector internet platform used most in British Columbia's schools is provided by Google. G Suite for Education ("GSFE") is a set of software applications that is provided to intermediary-users in the education industry on the basis of the Software as a Service arrangement described in Section 1.1.[52] G Suite for Education is also the brand name for the internet platform through which end-users access the software applications.

G Suite for Education provides a relatively long list of software applications. The extent to which these apps were designed or even customized for an education environment, however, is limited. This dynamic is illustrated in the Privacy Impact Assessment prepared by the Campbell River School District for use of the G Suite for Education platform.[53] The apps are as follows:

- Google Classroom
- Google Docs
- Google Sites
- Google Maps
- Google Photos
- Google Earth
- Google Mail (i.e. Gmail)
- Google Calendars
- Google Vault

The Campbell River School District thus intends for schools to make use of nine software applications through the GSFE platform. However, all but one of these applications are routinely made available to all Google users and are standard elements of Google's internet ecosystem. Indeed, Google's Docs, Sites, Maps,

[52] Jonathan Rochelle, "Introducing G Suite for Education" online: (October 2016) Google Education (blog) <https://blog.google/outreach-initiatives/education/introducing-g-suite-education/>. Google launched Google Apps for Education in 2006 and rebranded it as G Suite for Education in 2016.
[53] School District 72 - Campbell River, *Privacy Impact Assessment for Google Suite for Education (GSFE)* , online: <https://www.sd72.bc.ca/studentsparents/GSFE/Documents/GSFE%20PIA%20%20for%20SD72%20FINAL%20DRAFT.pdf>.

Photos, Earth, Gmail, Calendar, and Vault are collectively referred to as "Standard Google Apps" in the remainder of this report.[54]

In addition to the Standard Google Apps, Google Classroom is a learning management system that was originally developed specifically for GSFE. The primary function of Google Classroom is to structure the sharing of electronic documents between teachers and students. Google Classroom was first made available as a limited preview in May, 2014 and released to all GSFE users in August of the same year.[55] In 2017, Google Classroom was made available to all Google users as a free web service.[56] Google Classroom combines Google Drive, for assignment creation and distribution, with Google Docs, Google Sheets, and Google Slides for writing, and Gmail for communication. Over the years, Google has made incremental changes to Classroom. For example, in 2015, Google integrated Google Calendar into Google Classroom to facilitate scheduling of events such as assignment due dates, field trips and class speakers.[57] In 2018, additional new features and sections were added to Google Classroom with the grading interface reportedly improved. [58] Even more changes were announced in 2019 that have the cumulative effect of making Classroom more visually appealing. According to Google, Google Classroom "simplifies" the creation,

---

[54] For a survey on the use of cloud-based software applications and related skill development, see Hosam Al-Samarraie and Noria Saeed, "A Systematic Review of Cloud Computing Tools for Collaborative Learning: Opportunities and Challenges to the Blended-learning Environment" (2018) 124 Computers & Education 77-91. While assessing the pedagogical value of Standard Google Apps is not our focus here, it is hard not to wonder if the overall impact is to train young people in how to use Google's products..

[55]Darrell Etherington, "Google Debuts Classroom, An Education Platform for Teacher-Student Communication" online: (May 2014) TechCrunch <https://techcrunch.com/2014/05/06/google-debuts-classroom-an-education-platform-for-teacher-student-communication/>. See also Jordan Kahn, "Google Classroom now available to all Apps for Education users, adds collaboration features" online: (August 2014) 9TO5Google <https://9to5google.com/2014/08/12/google-classroom-now-available-to-all-apps-for-education-users-adds-collaboration-features/>..

[56] Darrell Etherington, "Google Classroom Now Lets Anyone School Anyone Else" online: (April 2017) TechCrunch <https://techcrunch.com/2017/04/27/google-classroom-now-lets-anyone-school-anyone-else/>.

[57] Lauren Hockenson, "Google Classroom Updates with Calendar Integration, New Teacher Tools" online: (August 2015) The Next Web <https://thenextweb.com/google/2015/08/24/google-classroom-back-2-school/>.

[58] Ope Bukola, "Time for a refresh: Meet the new Google Classroom" online (blog) (August 2018): Google Education < https://www.blog.google/outreach-initiatives/education/time-refresh-meet-new-google-classroom/>.

distribution, and grading of assignments so that paper documents are not necessary.[59]

Google's internet platform used by British Columbian schools, thus includes both a specific learning management system, i.e. Google Classroom, and a wide range of Standard Google Apps available to educational users.

2.2.b.ii Microsoft

Within the education technology market, the primary competitor to Google is Microsoft Corporation, which markets a product line called "Microsoft 365 Education."[60] Microsoft 365 Education is made up of three pricing plans that are referred to as A1, A3, and A5. A1 is the basic plan and is free for an unlimited number of individual users.[61]

Compared to Google, a noteworthy difference is that Microsoft 365 Education does not provide a specific learning management system. Google Classrooms, as noted above, has been modified over a series of iterations in order to meet the demands of K-12 classrooms. Microsoft Teams is the software application that is most similar to Google Classroom, but it was described by teachers during consultation for this project as "corporate-focused" and "less user-friendly."[62]

The key similarity between Microsoft and Google is that Microsoft also offers software applications that are accessed through an internet platform and hosted on the company's public cloud. Microsoft also does not negotiate service agreements with intermediary users in the education sector. Instead, Microsoft simply offers licenses to Microsoft 365 Education on a take it or leave it basis where the school board, as intermediary-user, must accept Microsoft's terms and

---

[59] Google for Education, Teacher Center, online <https://teachercenter.withgoogle.com/first-day-trainings/welcome-to-classroom>.

[60] Microsoft Education, *Microsoft 365 Education*, online <https://www.microsoft.com/en-ca/education/buy-license/microsoft365>.

[61] Microsoft Education, *Microsoft 365 Education*, online <https://www.microsoft.com/en-ca/education/buy-license/microsoft365>. Education institutions that choose to pay for either A3 or A5 are provided additional features.

[62] Teacher with Vancouver District School Board, public consultation held in Richmond B.C., Nov. 6, 2019.

conditions in order to use the platform.[63] Google's G Suite for Education is also only made available to users that accept its policies, which has resulted in concerns around "privacy by policy".[64]

2.2. b.iii FreshGrades

Although not the focus of this report, a number of interesting contrasts are raised by considering a product called FreshGrade Education, Inc. (FreshGrade). FreshGrade is a Canadian company that is headquartered in Kelowna and used in several British Columbian school districts.[65] FreshGrade's primary product is a learning management system with the following four core functionalities: (1) database of activities to be used in classroom lessons; (2) curation of digital portfolios; (3) exchange of multimedia messages; and (4) storage of score-based or standards-based evaluation. These general functionalities are also available through Google Classroom.

Nevertheless, there are noteworthy differences between FreshGrade and Google Classroom. First, FreshGrade is not made available for free. Instead, FreshGrade attempts to negotiate trials and license agreements with individual school districts. [66] Second, FreshGrade publicly places an emphasis on data privacy, and data that the company collects is stored on a Canadian cloud. Third, FreshGrade empowers parents and guardians to observe classroom activities, whereas

---

[63] Microsoft Education, *Microsoft in Education*, online <https://www.microsoft.com/en-ca/education>.

[64] Gennie Gebhart, "Privacy by Practice, Not Just by Policy: A System Administrator Advocating for Student Privacy", online: (2017) Electronic Frontier Foundation <https://www.eff.org/deeplinks/2017/03/privacy-practice-not-just-policy-system-administrator-advocating-student-privacy>. See also Alysia Lau, "The Privacy Box: Enabling Consumer Choice And Meaningful Consent In Online Privacy", online: (June 2017) The Public Interest Advocacy Centre <https://www.piac.ca/wp-content/uploads/2017/08/PIAC-THE-PRIVACY-BOX-OCA-REPORT-June-2017-ENG-FINAL.pdf>.

[65] Diane Strandberg, "8 Things to Know for Back to School in SD43" online: (September 2018) Tri-City News <https://www.tricitynews.com/news/8-things-to-know-for-back-to-school-in-sd43-1.23419109>. According to Strandberg "More parents [in district 43, which comprises Coquitlam, Port Coquitlam, and Port Moody] will be seeing their child's work on a digital portfolio called FreshGrade this year."

[66] Diane Strandberg, "8 Things to Know for Back to School in SD43". Strandberg reports that the School District pays a $45,000 annual licence fee for FreshGrades.

Google Classroom's focus appears to be on assisting teachers with workflow and classroom management.

Our consultations revealed that other private sector software applications are widely used on an *ad hoc* basis. Participants in the consultations indicated that reasons for *ad hoc* usage included both personal preference by individual teachers and traditions, within specific schools, of using a given application.[67] This is illustrative of a broader practical challenge whereby districts, schools, and teachers all have potentially divergent priorities about which software applications are used in the classroom. This, in turn, suggests that privacy is not the only lens through which it may be necessary to do further work on coordinating the interests of divergent stakeholders.

2.3 Use of Google's G Suite for Educations

As we turn to the specific case of Google, it is instructive to situate G Suite for Education in the broader Google Education marketing campaign. Google Education consists of two channels through which Google markets its overarching internet ecosystem. The first of these channels is the Google ChromeBook ("ChromeBook"). ChromeBook is an inexpensive laptop that, very generally speaking, is designed so that users run applications directly from the pre-installed, Google web browser rather than having the software installed on and run from the machine's hard drive. In turn, Google's own description of G Suite for Education as stated in a 2016 press release describes the product as a set of apps and extensions designed for compatibility with the company's Chrome internet browser.[68] The perceived result was described by a parent during consultations in Surrey: the fundamental purpose of G Suite for Education is to bring future internet users into Google's internet ecosystem, which is structured around the company's browser and its leading position in search algorithms.[69] This, in turn, is

[67] Parent of children in Langley District School Board schools, public consultation held in Richmond B.C., Nov. 6, 2019.

[68] Jonathan Rochelle, "Introducing G Suite for Education". Apps are software programs that are accessed through the browser, whereas extensions are software programs that modify the function of the browser. Apps are software programs that are accessed through the browser, whereas extensions are software programs that modify the function of the browser.

[69] Parent of children in Coquitlam District School Board schools, public consultation held in Surrey B.C., Nov. 7, 2019.

the outward manifestation of Google's advertising-centered business model that seeks to monetize users' attention.

When G Suite for Education was first launched in 2006, many of the early adopters were universities seeking to outsource email services. At that time, it was typical for Google to enter into a service contract whereby Google was the vendor and the university was a purchaser of services. Presently, Google no longer enters into a contract either with universities or with K-12 institutions. Instead, Google offers a strict set of terms that incorporate acceptance of the company's Privacy Policy. The result has been described as "Privacy by Policy" and is considered in later sub-sections of this report.[70] Since 2006, there have also been incremental proliferations of the number and types of software applications made available through the GSFE platform.

At least ten British Columbian school districts have created accounts with Google's G Suite for Education. Of course, it is not surprising that Google is a preferred provider of software applications in the province. As the world's largest internet company, Google has a number of apparent advantages, including:

- Products that are offered to school districts free of cost;
- Familiarity with the Standard Google Apps that may already be used by students and teachers;
- Users that access Google services through a GSFE credential are not directly subjected to advertising by Google;
- Partially customizable settings for the GSFE account and associated credentials that can be tailored by a local information technology administrator through an easy to use dashboard;
- Considerable data security investment that is an offshoot of Google massive operational scale.

The remainder of this section introduces the details of how Google's software application and the GSFE internet platform are being used in British Columbian schools.

[70] Gennie Gebhart, "Privacy by Practice, Not Just by Policy"

We were not able to find a centralized source of province-wide data on the use of G Suite for Education in British Columbia.[71] However, documentary and anecdotal information reviewed for this report provides some evidence of how Google is being used today in British Columbian schools. Documentary resources obtained for this report through freedom of information requests and internet research include: Privacy Impact Assessments ("PIAs") prepared at the district level; letters to guardians (i.e. requesting consent) that have filtered in to the public domain; and public-facing websites maintained by schools or school districts that describe the use of G Suite for Education in the classroom. Based on all of these sources, we conclude that, though it does not appear that every school or school district is using Google, many school districts in all parts of the province intend to or already have created G Suite for Education accounts.

The first step in using G Suite for Education is identifying a designated administrator at each school who then creates an account on behalf of the school on a Google-hosted web page for the G Suite for Education service/product.[72] This web page is referred to as a platform because it provides a base for users to access software applications. Once the administrator creates the school's G Suite for Education account, they then gain access to a settings page for the user side of the platform. This settings page, which is also referred to as a dashboard, enables the administrator to set preferences such as advertisement blocking and content filtering for the users associated with the school's account. Where the school has already arranged to have its own web domain, such as YourLocalSchoolNanaimo.ca, that address will be included during the above registration process with Google. As a result, Gmail accounts created for users through GSFE can be associated with the school's web address, e.g. Student1@YourLocalSchoolNanaimo.ca.)

[71] Craig Desson, "As Google for Education Tools Enter Classrooms Across Canada, Some Parents are Asking to Opt-out" online: (June 11, 2018), CBC Radio <https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935/as-google-for-education-tools-enter-classrooms-across-canada-some-parents-are-asking-to-opt-out-1.4694939>. Accessed 7-5-20.

[72] Google, *GSuite for Education*, online: <https://edu.google.com/products/gsuite-for-education/?modal_active=none&gclid=EAIaIQobChMIgYC0gfqi6QIVBNvACh3n1QCJEAAYASAAEgIcx_D_BwE>.

2.3.a Patterns in School Boards Intended Use of G Suite for Education

According to our research on the use of GSFE by school districts across the province, five patterns are visible. First, all of the school districts describe the use of GSFE as not being an educational requirement for students. Second, school districts are taking a formalistic approach to ensure that the software is used only for educational purposes. Third, within a given school district, differentiated access to the various software applications depending on students' grade level is anticipated; however, there is no consistent 'standard' on how much access should be given at what age or at which grade level between school districts. Fourth, there is no consistent approach to which of the Standard Google Apps will be used in the classroom; however, all of the school districts who have signed-up for GSFE provide teachers the option to use Google Classroom. Lastly, the school districts' usage intentions for both the Standard Google Apps and Google Classroom often reflect, nearly word by word, the uses that are promoted in Google's marketing material.

1. "No obligation" for students to Use Google

According to the public statements of the school districts, whether in the form of a PIA, a consent form sent to parents, or an announcement online, the message from the school district is consistent: students are not obligated to use any of the software on GSFE, and all school activities that rely on the use of these digital tools must allow for and accept alternate and equivalent means of student participation. In practice, however, there is little evidence that reasonable alternatives are offered by school districts. In the limited number of cases where parents are known to have refused to provide consent, questions persist about whether the relevant school districts have provided an alternative and equivalent means of participation for the student.[73] Furthermore, where the use of Google Classroom by teachers is institutionalized, there is a clear conflict between the teacher's interest in using the same administrative tools for all students, and the

[73] See for example, Craig Desson, "As Google for Education Tools Enter Classrooms Across Canada, Some Parents are Asking to Opt-out" online: (June 11, 2018), CBC Radio <https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935/as-google-for-education-tools-enter-classrooms-across-canada-some-parents-are-asking-to-opt-out-1.4694939>. Accessed 7-5-20.

family's interest in not being included in Google's system. A number of school districts have thus chosen to explicitly describe "the purpose" of G Suite for Education to be an "'educational use' to better meet the needs of students who are learning in a digital age".[74]

2. Form over substance when protecting privacy

School districts create policies that state that the software applications are used only for educational purposes and, concurrently, that sensitive and personally identifiable information should not be inputted into GSFE. The school board thus distributes a policy stipulating that the GSFE Software Applications should only be used for "educational purposes". This document is alternately called a "School District Use Policy" or "Use Policy". An illustration of this approach can be found under the "privacy" section of the Google Apps for Education (which was an earlier brand name of G Suite for Education and is sometimes referred to as GAFE) website maintained by the Kamloops/Thompson School District. The policy states that:

> The use of GAFE by SD73 staff and students is bound by the Kamloops/Thompson School District Information System Acceptable Use Procedure (as found in our online policy manual). As an overview, these documents state that users will conduct themselves in a courteous, ethical and responsible manner while using all district technology resources, including the SD73 GAFE platform.
>
> Personal account information and any created or uploaded content is hosted by Google in the US therefore there are important limitations to the type of information that can be shared within the SD73 GAFE system.
>
> *Both staff and students must remember that the purpose of the GAFE tools are for 'educational use'; to better meet the needs of students who are learning in a digital age. Therefore any and all*

[74] School District 72 - Campbell River, *Privacy Impact Assessment for Google Suite for Education (GSFE)*,

> *steps must be taken to ensure that sensitive and personally identifiable information is not shared in any emails, files and documents created or uploaded into the GAFE system.*[75]

On the basis of this type of policy document, the existing PIAs for GSFE assume that only limited amounts of personal information will be collected through student use of the GSFE software applications.

In addition to the policy documents, school districts are asking students' guardians to sign consent forms for the use of GSFE stipulating that the student will only use GSFE for educational purposes. The motivation for the Use Policy and consent form clearly appears to be a recognition that for the purpose of British Columbia's public sector privacy law (FOIPPA) personal information is being collected by or for the school district through the GSFE platform.[76] However, it is much less clear whether the language above satisfies the requirements of FOIPPA for informed consent. Indeed, the ultimate impact of these policies appears to shift the burden of compliance to individual households and, in some cases, to students themselves.

3. Differentiated Access

A third noteworthy pattern is that different classes of users will have different types of access to software applications through the GSFE platform. The simplest example of this is the distinction between the level of access granted to teachers and that granted to students. Specifically, students have more limited access to Google Classroom than teachers. For instance, a student can submit assignments and see his or her own grades but teachers, however, have access to a wider range of functionalities, such as lesson planning. Also, teachers can see the grades and assignments of all students whereas students can only see their own grades and work. Furthermore, the scope of access to the Standard Google Apps is

---

[75] School District No. 73 Kamloops/Thompson "Acceptable Use Guidelines", online: Google Apps for Education, <https://sites.google.com/a/gedu.sd73.bc.ca/sd73gafe/privacy/acceptable-use-guidelines>.
[76] An anecdotal example has appeared in widely circulated media, such as *The Atlantic*. Taylor Lorenz, "The Hottest Chat App for Teens Is … Google Docs" (Mar 14, 2019) The Atlantic online: <https://www.theatlantic.com/technology/archive/2019/03/hottest-chat-app-teens-google-docs/584857/>.

different based on a student's grade level. To cite one example, the Victoria School District anticipates that elementary school and secondary school students will have distinct levels of access as shown in Table 2.

Table 2: Grade Level Differentiated Use Policy in Greater Victoria

Students Kindergarten to Grade 8	Students Grade 9 - 12
GAFE email account is limited to only the SD61 or SD63 domains (@sd61learn.ca and @sd61.bc.ca, @sd63.bc.ca)	GAFE email account is not limited
Google Drive (unlimited storage, including docs, sheets, slides, forms, and drawing)	Google Drive (unlimited storage, including docs, sheets, slides, forms, and drawing)
Ability to share data is set to private by default	Ability to share data is set to private by default
Google Drive is limited sharing to only within the SD61 or SD63 domains	Google Drive sharing is not limited
Additional filtering and flagging in GAFE for inappropriate content	Additional filtering and flagging in GAFE for inappropriate content
Limited Google Apps for Education suite of products and services	Complete Google Apps for Education suite of products and services

[source: Victoria PIA]

It is relatively common for school districts to provide differentiated access based on students' grade level; however, there is no consistent standard between school districts regarding how much access should be given at a certain grade level. Furthermore, in the absence of a GSFE credential, Google does not allow children under 13 years of age to register for its services.[77]

[77] Google, "Age Requirements on Google Accounts" online: <https://support.google.com/accounts/answer/1350409?hl=en>.

4. Inconsistent Parameters regarding which Software Applications are used

The case of Victoria also helps to illustrate a fourth pattern, which is that not all of the Standard Google Apps are being used. For instance, according to consent forms given to students and published by the CBC, the only apps being used in Greater Victoria are GMail, Google Drive, Google Calendar, Google Sites, and Google Classroom.[78] In West Vancouver, meanwhile, parents have been informed that students will be given access to a similar, but not identical, conscripted list of Apps, i.e.: Google Mail, Google Drive, Google Docs, Google Calendar, and Google Classroom.[79]

5. Influence of Google Marketing

Finally, the school districts' intended use for both the Standard Google Apps and Google Classroom often reflect, almost word by word, the uses that are promoted by Google through its Google Education marketing campaign. For example, the Nanaimo school district's PIA lists the apps that will be made available to local schools and, in theory, how these apps will be used:

- Google Docs: Personal Narratives, Fictional Stories, Paragraph Writing, Internet Safety Presentations, Word Definition Presentations for Word Studies, Student-led Conference Presentation, Forms for Quizzes for Language Arts, Reading, Science and Social Studies and online note-taking using custom made Google Forms
- Google Sites: Student ePortfolios, Local Research Projects, Collaborative Science Research;

[78] Craig Desson, "As Google for Education Tools Enter Classrooms Across Canada, Some Parents are Asking to Opt-out" online: (June 11, 2018), CBC Radio <https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935/as-google-for-education-tools-enter-classrooms-across-canada-some-parents-are-asking-to-opt-out-1.4694939>. Accessed 7-5-20. Desson reproduces the Greater Victoria School District's "Information Letter & Permission Form". See also, Greater Victoria School District, *Privacy Impact Assessment for School District No. 61 (Greater Victoria) and School District No. 63 (Saanich)* (2018), online: <https://www.sd61.bc.ca/wp-content/uploads/sites/91/2018/09/GSuite-PIA-SD61_63.pdf>.

[79] West Vancouver School District, "Information Letter & Permission Form"

- **Google Maps:** Social Studies, Provincial First-nations Studies Projects, and Mapping Places in British Columbia and Recording Elevation Profiles on BC Destinations;
- **Google Photos:** Classroom Picture Editing, Presentation Creation, Subject Topic Catalogues and Field Trip Documentation
- **Google Earth:** 3-D Exploration of the earth, Castles, Cathedrals and World Museum Trips, Geography Tours, Literature Trips
- **Gmail:** Communication with students, Book Club Communication, Reader Response Journals
- **Google Calendars:** Organization of classroom projects, assignments and school events
- **Google Vault:** Archiving and eDiscovery for GSFE[80]

Looking at the above list in light of other PIAs and Google's sales material, it is apparent that this is boiler plate language. In fact, the wording is an almost exact reproduction of Google's GSFE sales material. The issue of Google's influence over the way in which usage is conceptualized is also examined section 2.4 on training material.

2.3.b Flow of Information Within Google's System

Questions naturally arise about where and how information is intended to flow within the system. The notion of a system, in this case, has at least two complimentary meanings. First, there is the massive, global information management system maintained by Google. Second, there is the local system constituted by six types of actors: student guardians, students, public bodies, Google, Google's third parties, and internet service providers. For present purposes, we focus on the first system, which is to say the interlinkage of Google's internet-based software applications, the storage of the information running through these applications at Google's digital cloud farms.

When the school creates a school-level account with G Suite for Education, the school administrator gains access to the GSFE dashboard where they can create user profiles for students. The creation of these user profiles opens the gate for

[80] Nanaimo Ladysmith School District, *Privacy Impact Assessment for School District No. 68*, online: <https://www.sd68.bc.ca/wp-content/uploads/GSFE_PIA_NLPS.pdf>.

the flow of student information into the Google system. This takes place in four stages.

The first stage begins when schools send a consent form to each student's household. If the consent form is returned to the school, then the student's name, student number, school, and grade will be inputted into Google's system. Gender and age are not directly provided to Google at this stage. As a by-product of establishing a GSFE user profile, a Gmail account is created for the student.

The second stage in the flow of information results from the actual usage of the GSFE software applications by each student. Specifically, when a student logs in to his or her GSFE user profile, Google's user log is activated and begins to track the user's internet behavior. So, for instance, if the student logs in to his or her GSFE-associated Gmail account to check for a message from a teacher or classmate, then that information flows into the Google system. If the student proceeds to use Google Earth to review maps for a geography assignment, that information is also logged into Google's system. If the student reviews videos about that same country – for example, Portugal – through YouTube, that information also flows into Google's system. The Nanaimo district school board's letter to parents and guardians seeking consent summarizes the information that will flow into the Google system, for example, as follows:

1. Student's name, grade level and school name to create the GSFE login account
2. Classroom assignments, research notes, presentations, school-based projects
3. Multimedia objects created by students (videos, pictures, audio files, animations, etc.)
4. Quizzes, tests, surveys
5. Professional development materials and documents
6. Summative assessments (e.g., teacher comments, peer feedback)
7. Calendars for assignment dates, project deadlines, events
8. Communication with teachers and other students related to educational purposes

9. Images and video of students for educational purposes.[81]

There is, therefore, an attempt in items 8 and 9 to stipulate that only information related to educational purposes will be collected and stored by Google. However, frankly and practically speaking, information created by students will be collected and stored by Google's cloud computing system regardless of its purpose for creation.

For current purposes, it is useful to distinguish analytically between information generated for an educational purpose and information that has no connection to the classroom. The third stage in the flow of student information occurs where a student remains logged-in to the GSFE credential but starts using the resource for purely personal purposes. For example, the student described above may decide that he or she needs a break from the geography assignment and tune in to videos on YouTube that are no longer about Portugal but instead about topics that are – according to Google's algorithm – relevant. For example, these could include Portugual's national soccer team or its star players. All of the information generated by Google about these usage patterns flows into Google's system. So long as a student remains logged in to their GSFE credential, Google will continue to track the browser's activity and associate that behavior with the student even after the student closes their device or discontinues using the internet. Because all this activity is associated with the student's name, there is credible grounds to believe that it is personal information.

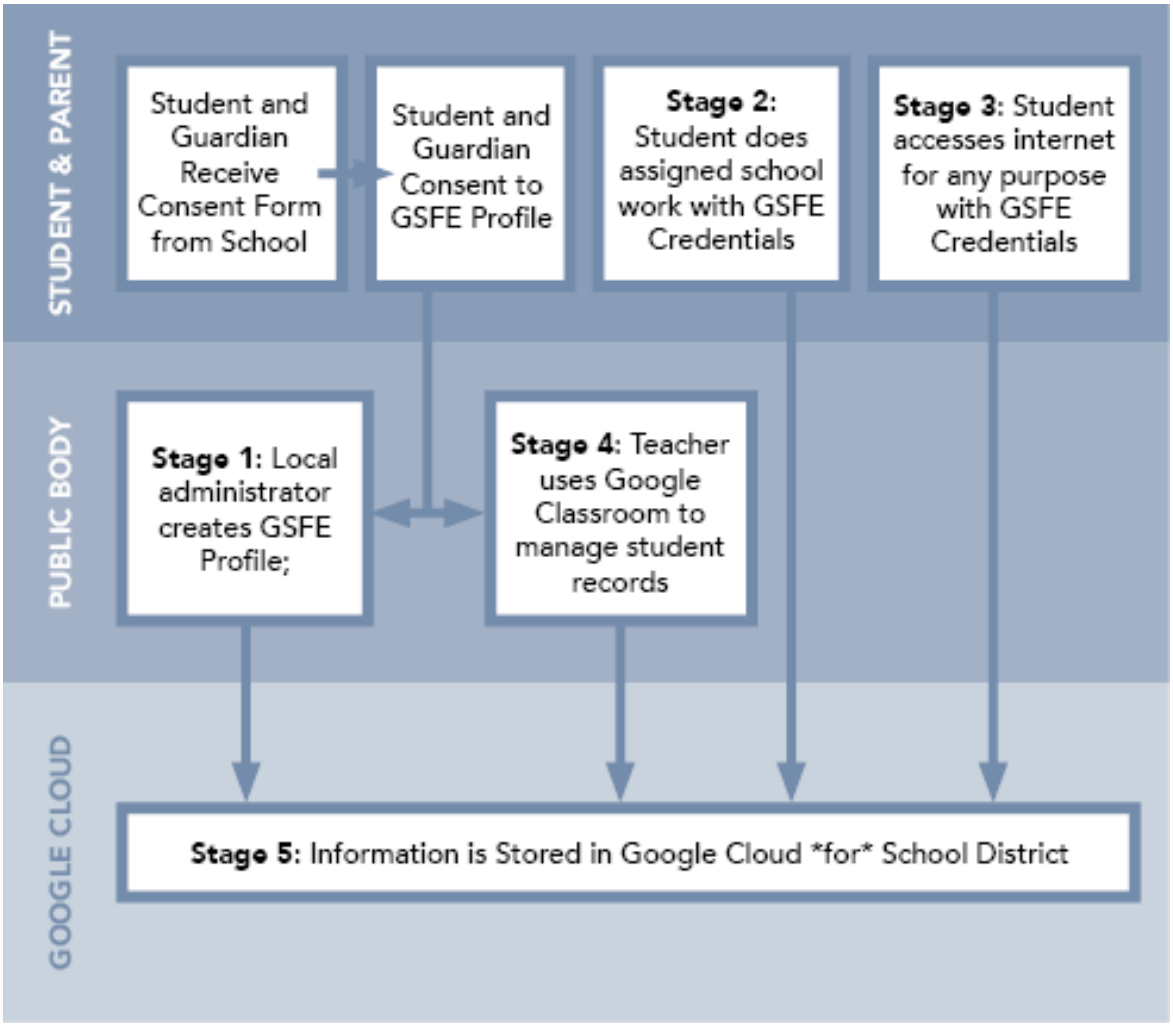
The fourth stage in the flow of information is enabled by the learning management system, i.e. Google Classroom, that is included in the GSFE platform. At this stage, it is not the student, but rather the teacher, who is inputting information into the system. A core functionality of Google Classroom is called "Grade Book" which is an easy-to-use database for teachers to record grades, other forms of evaluation, and feedback for students. Google Classroom's Grade Book also stores the students' work that is the subject of evaluation. As a general rule, this means that work submitted to a teacher in a GSFE classroom and teacher

[81] Nanaimo Ladysmith School District, *Information Letter & Permission Form* (2015), online: <https://www.sd68.bc.ca/wp-content/uploads/Consent-Form.pdf>.

evaluation of that work will be uploaded to Google's platform on the internet, and as explained below, it will then be stored in Google's digital cloud.

The fifth stage in the flow of information is that information inputted into the software on the GSFE platform is ultimately stored in the cloud. This means that the digital data created by the software is not on a specific device but rather stored on a network of servers which are distributed across the relevant cloud architecture. In the case of Google, the supercomputer farms that run Google's cloud are in over twenty different geographical hubs, with the closest one to British Columbia being in Oregon. Although there are commercial incentives for Google to store data at cloud hubs that are proximate to where it is collected and subsequently used, there is no guarantee that information collected through the GSFE platform will only be stored at Google's Oregon data centre.

Table 3: Flow chart of student information in Google's system



2.4 Training materials prepared by Google, School Districts, and the Provincial Government

This section reviews training materials prepared by Google, school districts, and the provincial government. It finds that Google has been very successful at establishing the terms through which its products are discussed by educators in British Columbia.

Google Education is a campaign that markets hardware and software to education institutions. Google Education has directly and indirectly produced a massive volume of content, including training materials, that demonstrate how the use of GSFE can be integrated into what the company describes as a "21st century classroom".[82] Google has not, however, prepared any training materials specifically for British Columbian schools. Instead, it uses a 'train the trainer' model whereby it licenses education consultants who then provide their services, often on a commercial basis, to classroom educators. The result is a cluster-effect in the educational technology industry where specialists have often been trained or licensed by Google.

Two themes are particularly noteworthy in the training materials prepared by Google for K-12 institutions. First, Google highlights "[t]ools for collaboration, communication, and creativity," as the primary pedagogical benefits of using the G Suite for Education platform. The notion of software as "tools" is a manifestation of the Google worldview. With these tools, it is proposed that, "Students can learn 21st-century problem-solving and the skills they'll use in their future careers."[83] This metaphor of software as a tool, which implicitly suggests that software is a tool for the manipulation of symbols, is reminiscent of the notion of 21st century workers as "symbolic analysts", which was proposed by former U.S. Secretary of Labour Robert Reich as a solution to de-industrialization and under-employment.[84] A second core appeal made by Google is that its cloud-based internet ecosystem, "[will] allow both educators and students to work on tasks on

[82] Google, *Teacher Center*, online: <https://teachercenter.withgoogle.com>.
[83] Google, *Teacher Center*, online: <https://teachercenter.withgoogle.com>.
[84] Robert Reich, *The Work of Nations: Preparing Ourselves for 21st Century Capitalism* (New York: Knopf, 1992). Reich served as U.S. Secretary under Bill Clinton.

any device and from any place."[85] Indeed, the idea of "working" from any place on any device is central to Google's vision of a place-less internet that can be accessed by a geographically dispersed population in order to exchange data.

Several school districts have created public websites with materials on GSFE. For instance, School District 73 in Kamloops/Thompson uses Google Sites to create a page that introduces, in very general terms, the notion of cloud-based software applications and identifies the applications within GSFE that are used by schools in the district. The page also contains links to various training resources created by Google Education.[86] Two school districts in particular have posted materials with more substantial training content. One of these is the Greater Victoria School District, which notes on its Technology for Learning webpage that:

> Since consent for GSuite is a requirement for participation, teachers need to carefully consider what alternative accommodations they will provide to students that do not have consent for its use. Accommodations will vary depending on how GSuite is used in the classroom. Student classroom participation cannot depend upon use of GSuite which is why accommodations are a necessary component to GSuite integration in any classroom.[87] [emphasis added]

The same Technology for Learning webpage then goes on to identify specific accommodations for each software application that is being used within the district. It should also be mentioned that the resource page created by the Victoria school district provides materials for teaching students about privacy.

A second district that has taken a proactive approach to disseminating information about GSFE is Delta. In particular, the Delta school district has taken the initiative to create a presentation on the appropriate usage of GSFE that explains in non-

---

[85] British Columbia Ministry of Education, "G Suite for Education 2018", online: (2018) Special Education Technology BC <https://www.setbc.org/2018/05/g-suite-for-education/#1447962038934-6da3c7fa-17p5>.
[86] School District No. 73 (Kamloops/Thompson) "Access to Google Applications for Education Accounts", online: Student Enrollment Form <https://sites.google.com/a/gedu.sd73.bc.ca/sd73gafe/privacy/who-can-access-my-information>.
[87] Greater Victoria School District, "Accommodations", online: Technology for Learning <https://techforlearning.sd61.bc.ca/privacy/g-suite-edu/accommodations/>.

technical language why students should consider their own and other people's privacy when using the tools provided by Google.[88]

As of December 2019, the provincial government's primary channel for creating and distributing training materials about Google's products has been Special Education Technology – British Columbia ("SET-BC"). SET-BC is an outreach program of the BC Ministry of Education that was established in 1989 to assist school districts in utilizing technology with special needs students, especially those whose physical access to schools is restricted. SET-BC offers facilitated in-person training and on-demand training around a wide range of pedagogical tools and issues. This includes a limited set of resources about the use of G Suite apps. Among these materials, SET-BC lists five software applications that are available through G Suite and that are identified as highly recommended. Those five software applications are Google Classroom, Google Docs, Google Forms, Google Hangouts, and Google Drive. The applications are introduced very briefly and the reader is guided to further resources that are almost all materials created by Google.[89] In general, the materials created by SET-BC do not consider privacy issues; however, one resource set regarding Google Classroom mentions as follows, "Since it is a cloud based system please make sure there is informed consent for using this platform."[90]

2.5 Zoom

On March 18, 2020, British Columbia declared a "state of emergency" under the *Emergency Program Act* in relation to the Covid-19 pandemic.[91] On the same date, the provincial government decided to close all public schools. The Minister

---

[88] Delta School District, *Learn at Home,* online: <https://deltalearns.ca>.

[89]British Columbia Ministry of Education, "G Suite Apps, Implementation Strategies, and Resources", online: (2018) Special Education Technology BC <https://www.setbc.org/download/Public/GSuite/G_Suite_Apps_Implementation_Strategies_Resources.pdf>.

[90] British Columbia Ministry of Education, "*Google Classroom* ", online: (2018) Special Education Technology BC <https://www.setbc.org/2018/10/google-classroom/>.

[91] Ministry of Public Safety and Solicitor General, "Province declares state of emergency to support COVID-19 response," (March 18, 2020) news release <https://news.gov.bc.ca/releases/2020PSSG0017-000511>.

of Education explained that: "We're used to schools being safe places …. We have to take action today to protect our students and staff."[92]

Closure of schools, however, raised concerns about continuity of learning and graduation. The need to shift to remote instruction was quickly recognized. Meanwhile, on March 26, 2020 the Minister of Citizens' Services issued a ministerial order pursuant to FOIPPA authorizing the relaxation of certain privacy safeguards related to the use of net-based platforms and applications by public bodies.[93]

On April 1, 2020 the Ministry of Education announced that it had licenced a popular video-conferencing software application called Zoom. According to the province, Zoom would support virtual learning for students from kindergarten to Grade 12 throughout the COVID-19 emergency. The Ministry of Education indicated in a press release that "[t]his will allow consistent access for educators who choose to use it, giving them more ways to communicate with students and parents."[94]

Of note, the licensing agreement was negotiated directly between the provincial Ministry of Education and Zoom, rather than being managed by individual school boards. Furthermore, the ministry indicated in its press release that To ensure safety and privacy for students, the licensing agreement complies with B.C.'s Freedom of Information and Protection of Privacy Act. … The Zoom server will be based in Canada, with added encryption so it is a safe platform to learn."[95]

The "Zoom Case" raises at least two types of legitimate questions.

---

[92] Kendra Mangione, "All B.C. public schools will be closed for now over COVID-19 concerns" (March 17, 2020) CTV News <https://bc.ctvnews.ca/all-b-c-public-schools-will-be-closed-for-now-over-covid-19-concerns-1.4856680>.

[93] *Ministerial Order No. M085* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085>; *Ministerial Order No. M180* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m180>

[94] Ministry of Education, "Zoom collaboration tool now available for K-12 continuous learning," (March 18, 2020) news release < https://news.gov.bc.ca/releases/2020EDUC0027-000608>.

[95] Ministry of Education, "Zoom collaboration tool now available for K-12 continuous learning," (March 18, 2020) news release < https://news.gov.bc.ca/releases/2020EDUC0027-000608>.

First, there are questions about whether the provincial government's negotiation of a license agreement with Zoom and guarantee that Zoom's server will be based in Canada creates a precedent for the procurement of information technology services in public schools

Second, there are questions about whether Zoom is in fact a suitable tool for public schools.

Zoom was not designed as an education technology product. Prior to the Covid-19 pandemic, Zoom had been used primarily by business as an alternative to Skype.

In Abbotsford, the district Superintendent has flagged security and privacy concerns around Zoom, and advised teachers not to use it. According to published reports, the letter to teachers reported that parents are "very concerned" about their children using Zoom and that "Zoom, with its weak security, and vague privacy policies has become a major target in recent weeks for bad actors to mine personal data, and this will continue to escalate over the next several weeks/months".[96]

In the United States, there has been considerable backlash against the use of Zoom by public schools. On April 6, 2020 the New York City Department of Education banned the use of Zoom by its public schools due to privacy and security concerns.[97] Los Angeles teachers have also stopped using Zoom due to a phenomenon known as "zoombombing" wherein intruders interrupted meetings with offence and hateful media.[98]

---

[96] Andrea Ross, "Abbotsford teachers not allowed to use Zoom video-conferencing licensed by province," (April 10, 2020) CBC News <https://www.cbc.ca/news/canada/british-columbia/abbotsford-schools-zoom-video-conferencing-1.5528556>.

[97] Lauren Camera, "New York City Tells Teachers to Stop Using Zoom for Distance Learning" (April 7, 2020) U.S. News & World Report <https://www.usnews.com/news/education-news/articles/2020-04-07/new-york-city-tells-teachers-to-stop-using-zoom-for-distance-learning>.

[98] Rosanna Xia, Howard Blume, Luke Money "USC, school districts getting 'Zoom-bombed' with racist taunts, porn as they transition to online meetings" (March 25, 2020) Los Angeles Times <https://www.latimes.com/california/story/2020-03-25/zoombombing-usc-classes-interrupted-racist-remarks>.

3. PRIVACY FRAMEWORK FOR BRITISH COLUMBIA PUBLIC SCHOOLS

Claims to personal privacy are often traced back to the 19th century's emergence of a public sphere alongside early forms of mass media, and the implicit contrast of public and private life. Since the middle of the twentieth century, three powerful conceptions of privacy have been articulated. Those conceptions are: (1) a "Surveillance Model"; (2) a "Capture Model"; and most recently (3) a "Datafication Model." In the last three decades, liberal democracies have also started to formulate and protect privacy rights through the law. In the 1980s, as Canada's federal and provincial governments began legislating fundamental rights befitting a mature democracy, privacy rights arrived in Canada. In British Columbia, the 1996 *Freedom of Information and Protection of Privacy Act* ("*FOIPPA*"),[99] which pertains to information held by the public sector, established individual rights concerning the collection, use, and disclosure of "personal information" by any public body. The following two sub-sections examine the growth in this area of the law and the importance of information privacy along with the protection of personal information. Then, the final section situates privacy rights in a legal and policy analysis of British Columbia's public education system.

3.1 Sources of Canadian Privacy Law

Public discourses on privacy are often traced back to an 1890 article by Samuel Warren and Louis Brandeis, who later served as a justice of the United States Supreme Court.[100] Warren and Brandeis argued that society must recognize a right to privacy, which they defined as "the right to be let alone."[101] Since then, numerous other individuals, organizations and multilateral fora have advanced

[99] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

[100] Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193. According to a leading Canadian text on privacy law, "[a]lthough they were American, their thinking on the issue of privacy was, and has been, equally influential in Canada.". Kris Klein, *Canadian Privacy: Data Protection Law and Policy for the Practitioner* (International Association of Privacy Professionals, 2009) at 6.

[101] Warren and Brandeis , "The Right to Privacy", at 195. Warren and Brandeis trace this right to technological change, especially the combination of mass-printing and photography that threatened to invade the "sacred precincts of private and domestic life."

their own conceptions of privacy. Indeed, the importance of privacy has been clearly recognized at the international level. For example, Article 3 of the *Universal Declaration of Human Rights* states that every person has the right to life, liberty and security of the person.[102] Article 12 of the *Universal Declaration* provides that, "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[103]

The intellectual history of privacy is beyond the scope of this report, but we can and do benefit from related scholarship. Research on conceptions of privacy since the end of the Second World War has found three models:

- A "Surveillance Model" that was focused on "the historical experience of secret police organizations and their networks of listening devices and informers".[104]
- The "Capture Model" that emerged as a response to "new technologies for the tracking of people, automobiles, packages, materials, and so forth" in the 1990s.[105]
- The "Datafication Model", which supplements the previous focus on the collection of information by shifting the focus of concern to data processing and analysis.[106]

These three models are applied in the analysis throughout this report.

Domestic legislation protecting personal privacy begins in 1970's West Germany.[107] This was both a response to local discourses within the Surveillance

---

[102] United Nations, *Human Rights: A Compilation of International Instruments* (New York: United Nations, 1978) at I. (UN Doc. ST/HR/I/Rev.1, Sales No. E.78.xlv.2)

[103] United Nations, *Human Rights: A Compilation of International Instruments* at 2. The International Covenant on Civil and Political Rights contains substantially identical principles.

[104] Philip E Agre, "Surveillance and Capture: Two Models of Privacy" (2010) 10:2 The Information Society 101 at 106.

[105] Agre, "Surveillance and Capture: Two Models of Privacy", at 107.

[106] Jens-Erik Mai, "Big Data Privacy: The Datafication of Personal Information" (2016) 32:3 The Information Society at 192-199 <https://www.tandfonline.com/doi/full/10.1080/01972243.2016.1153010>

[107] J L Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", online: (1983), 6 B.C. Int'l & Comp L Rev 243 <

Model – i.e. desire to prevent the abuses characteristic of Nazi and Communist Germany – and motivated by early concerns within the Capture Model as information technology systems began to proliferate. These same concerns about the increasing use of information technology circulated in 1970's Canada, but they did not immediately lead to legislation.[108] The subsequent growth of European privacy laws and demand that trading partners reciprocate also influenced the development of Canada's privacy laws, especially as they pertain to the private sector.[109]

In the 1980's, the Canadian government began legislating fundamental individual rights, with *The Charter of Rights and Freedoms* being an especially prominent example. During this same period, the Parliament of Canada also passed the *Privacy Act*[110] and the *Access to Information Act.*[111] In a nutshell, the Privacy Act sought to ensure that the federal government was meeting internationally accepted practices regarding the handling of personal information. Chief Justice McLachlin stated that:

> The *Access to Information* and *Privacy Acts* came into force together on Canada Day 1983 … not long after Canada adopted its *Charter of Rights and Freedoms*. It was a heady time for Canadian constitutional development. The country had just, after long travail and discussion, repatriated its constitution to make it truly independent and at the same time, enshrined in its

http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8>. In 1970, the West German state of Hessen passed the world's first such law, and in 1978 a national information privacy law came into force across West Germany.

[108] Canada Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force* established jointly by Department of Communications / Department of Justice (Ottawa: Information Canada, 1972)

[109] Under the European Union's 1995 Data Protection Directive, transfer of personal data to countries outside the EU was, in principle, only permitted if that country provided an adequate level of protection. In 2001, the EU recognized Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) as providing adequate protection. Note also the Organization for Economic Cooperation and Development's 1984 Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.' The Guidelines were intended to harmonize data protection laws and practices among OECD member countries by establishing minimum standards for handling personal information.

[110] *Privacy Act,* RSC 1985, c P-21.

[111] *Access to Information Act,* RSC 1985, c A-1. The two statutes cross-reference each other; for example, the definition of "personal information" in the Access to Information Act makes specific reference to the Privacy Act.

> constitution a powerful affirmation of rights. The capstone of this new constitutional edifice — less well known but nevertheless important — was the adoption of twin laws of quasi-constitutional status, aimed at protecting Canadians' right to access to information and privacy.[112]

Chief Justice McLachlin's words reflect the well-established legal principle that the right to privacy has a quasi-constitutional status in Canada.

Indeed, the provinces followed the federal government's broad agenda of establishing individual rights pertaining to access to information and privacy. However, the provinces typically legislated access to information and protection of privacy in a single statute. This drafting strategy was adopted in British Columbia's *Freedom of Information and Protection of Privacy Act.*[113] Section 2 of FOIPPA states that the purposes of the Act are to make the government more accountable to the public and to protect personal privacy.

It is also important to note the role of the Office of the Information and Privacy Commissioner ("Privacy Commissioner"), which was established in 1996 under FOIPPA. The Privacy Commissioner is an independent Officer of the Legislature with the responsibility of overseeing the application and enforcement of FOIPPA.[114] The OIPC's privacy mandate includes monitoring compliance with the Act,[115] investigating complaints under the Act,[116] and educating the public about the Act.[117]

The Privacy Commissioner's mandate to monitor compliance with FOIPPA merits attention. The relevant provision is FOIPPA s. 42., which stipulates that the Privacy Commissioner is "generally responsible for monitoring how this Act is

---

[112] Office of the Privacy Commissioner of Canada, *Privacy Act Reform in an Era of Change and Transparency* (2016), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322>.
[113] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.
[114] *FOIPPA,* s 37. See generally, *FOIPPA*, Part 4.
[115] *FOIPPA,* s 42.
[116] *FOIPPA,* ss 56, 58.
[117] *FOIPPA, s 42.*

administered to ensure that its purposes are achieved".[118] Pursuant to s. 42(1), the Privacy Commissioner is empowered to

- receive comments from the public about the administration of the Act,[119]
- engage in or commission research into anything affecting the achievement of the purposes of the Act,[120]
- comment on the implications for protection of privacy of proposed legislative schemes or programs or activities of public bodies,[121]

The Privacy Commissioner therefore has specific powers with regard to monitoring the achievement of the Act's purposes. The ability to comment upon the privacy implications of public bodies' programs or activities should help to ensure that the government is held accountable. This mandate is similar to that of an Ombudsperson and means that the Privacy Commissioner has a practice of issuing guidance documents on topical privacy issues.

Finally, as explained by the Commissioner, "[p]rivacy in democratic countries is protected by a mix of laws enacted by elected representatives and, often but not always, constitutional guarantees interpreted by the courts."[122] Over the last three decades, Canadian privacy law has undergone considerable growth and maturation. Canadian jurists primarily divide privacy into the following dimensions:

- Bodily privacy: Also sometimes called privacy of the person, this type of privacy protects bodily integrity. Privacy, in this sense, means protection of the individual against physical intrusions, such as physical searches by police, body cavity searches, drug testing, and genetic testing.
- Territorial privacy: This type of privacy places limitations on intrusions into an individual's physical environment. This conception of privacy can involve a right to protection against intrusion on one's property, such as one's

[118] *FOIPPA, s 42.*(1)
[119] *FOIPPA,* 42.(1) (d)
[120] *FOIPPA*, 42.(1) (e)
[121] *FOIPPA* , 42.(1) (f)
[122] Information & Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act* at 36

home. It may also pertain to a right to protection from surveillance by cameras, eavesdropping devices or even researchers.[123]

- Information privacy: This type of privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[124] Laws about information privacy are concerned with establishing rules about "personal information."

Our focus the remainder of this report is on information privacy.

3.2 Information Privacy and Personal Information

As introduced above, Canadian law protects three types of privacy: bodily, territorial, and information. All three are important; however, information privacy is of special importance for understanding the law generally and the use of software applications in the classroom more specifically. This section reviews the special importance given to informational privacy by Canadian law.

To fully appreciate why Canadian law gives informational privacy a privileged place, it is useful to take a step back and consider why democratic societies consider privacy a fundamental value in the first place. The British Columbia OIPC has observed that:

> The essence of liberty in a democratic society is the right of individuals to autonomy—to be free from state interference. The right to privacy has several components, including the right (with only limited and clearly justified exceptions) to control access to and the use of information about individuals. Although privacy is essential to individual autonomy, it is not just an individual right. A sphere of privacy enables us to fulfill our roles as community

[123] Kris Klein, *Canadian Privacy: Data Protection Law and Policy for the Practitioner*, (International Association of Privacy Professionals, 2009) at 7.
[124] AF Westin, *Privacy and Freedom* (New York:The Bodley Head Ltd, 1970) at 7.

> members and is ultimately essential to the health of our democracy.[125]

The above introduces the essential distinction between information and personal information. An essential foundation for understanding Canadian privacy legislation is thus the concept of personal information.[126]

According to the Privacy Commissioner of Canada, personal information is "information that on its own or combined with other pieces of data, can identify *you* as an individual."[127] In other words, personal information is information – data - about an identifiable individual.

Personal information is a defined term in British Columbia's *FOIPPA*. Section 1 of *FOIPPA* states that, "'Personal information' means recorded information about an identifiable individual other than contact information".[128] Furthermore, personal information under *FOIPPA* includes "not only basic identifying details (such as name, address, phone number, ID numbers, blood or other body tissue type), but also information related to a person's life history (such as medical or educational information, employment information, political beliefs or religious associations)."[129]

In order to fully appreciate the scope and significance of this key term for Canadian privacy law, including *FOIPPA*, we need to acknowledge jurisprudence from the Supreme Court of Canada.

The seminal Supreme Court of Canada case on the interpretation of the term "personal information" is *Dagg v. Canada*.[130] In *Dagg*, the appellant was a human

---

[125] Information & Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act,* at 13.

[126] Both the federal Privacy Act and BC's FOIPPA provide a single level of protection for all types of personal information.

[127] Office of the Privacy Commissioner of Canada, *Summary of Privacy Laws in Canada* (January 2018), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>.

[128] *FOIPPA*, Schedule 1.

[129] Information & Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act,* at 4.

[130] Dagg v. Canada (Minister of Finance), 1997 CanLII 358 (SCC), [1997] 2 SCR 403. Note that the statute under consideration was the federal Privacy Act, which defines personal information as information about an identifiable individual that is recorded. This is sufficiently similar to the FOIPPA definition to make the Dagg decision controlling in British Columbia.

resources consultant who sought to access departmental sign-in logs for after-hours work at the Ministry of Finance. The Minister refused to disclose portions of the logs on the basis that the information constituted personal information under the federal *Privacy Act*. The careful and extensive reasons of Justice La Forest in *Dagg* offer a road map for interpreting the term "personal information". La Forest J's reasoning clarifies that the primary consideration in assessing whether a particular piece of information is personal information is whether that information results in the individual being identifiable. The result is that the definition of personal information in the *Privacy Act* is expansive, "deliberately broad" [131] and "entirely consistent with the great pains that have been taken to safeguard individual identity. Its intent seems to be to capture any information about a specific person, subject only to specific exceptions."[132] In arriving at this interpretation, Justice La Forest re-affirmed that in Canada, privacy is a quasi-constitutional right, stating that:

> [P]rivacy in relation to information … is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): 'This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.'[133]

In fact, as introduced above via the public comments of Chief Justice McLachlin, the Supreme Court of Canada treats a limited set of statutes as quasi-constitutional. This includes human rights, privacy and official languages legislation, and statutory bills of rights such as the *Canadian Bill of Rights* and the Quebec *Charter of Human Rights and Freedoms*. Although these statutes were enacted in the same manner as ordinary legislation, their quasi-constitutional status requires that they are interpreted in a broad and generous manner. The

---

[131] *Dagg* at para 52 . Reference to Jerome ACJ in *Canada (Information Commissioner) v Canada (Solicitor General)*, [1988] 3 FC 551 (72).

[132] *Dagg*.

[133] *Dagg at para 67* . Reference to *R v Dyment*, [1988] 2 SCR 417 at paras 429-30.

quasi-constitutional nature of the federal *Privacy Act* has been repeatedly affirmed by the Supreme Court.[134]

Although British Columbia's public sector act has not been explicitly considered by the Supreme Court, a recent case regarding Alberta's private sector privacy act, the *Personal Information Protection Act* ("Alberta's PIPA") is instructive. The case involved a labour union's collection and use of members' personal information without consent. The labour union claimed that the restriction under Alberta's PIPA from engaging in such conduct resulted in a violation of its *Charter* right to freedom of expression.[135] The Supreme Court found that:

> [t]he ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society.[136]

In this respect, it is also important to note Section 79 of *FOIPPA*. *FOIPPA* S. 79 provides that if a provision of *FOIPPA* is inconsistent or in conflict with a provision of another Act, the provision of *FOIPPA* prevails unless the other Act expressly provides that it, or a provision of it, applies despite *FOIPPA*.[137] The Information and Privacy Commissioner of British Columbia has thus observed that, "[l]ike human rights legislation, *FOIPPA* generally overrides any other conflicting provincial legislation."[138]

---

[134] *Lavigne v Canada (Office of the Commissioner of Official Languages),* [2002] 2 SCR 773, at para 24*; Heinz Co. of Canada Ltd. v Canada (Attorney General),* [2006] 1 SCR 441, at para 28.

[135] *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62.

[136] *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

[137] *FOIPPA, s. 79.*

[138] *Privacy and the USA Patriot Act,* at 97

How, then, should children's personal information be protected when using internet platforms and software applications in British Columbia classrooms? We examine this question and potential answers from the perspective of privacy law, public policy, and ethics. The following sub-section reviews the *School Act* in order to provide an important piece of context about the public education system and the inter-related roles of schools, districts, and the provincial ministry.

3.3 Public Education System

This section provides a law and policy overview of British Columbia's public education system. In particular, it uses the *School Act* to provide the reader with a schema for understanding the intersecting roles of two key actors, i.e. the provincial Minister of Education and local Boards of Education. Indeed, scholars note that British Columbia's public education system reflects a fundamental bargain between provincial oversight and local representation.[139] In addition to the Minister and the Boards, it is important to recognize the essential role of stakeholders such as students, parents, and teachers, in the public education system.

Canada's Constitution provides the provinces with exclusive jurisdiction over education.[140] This includes the organization, delivery, and assessment of education at the elementary and secondary levels, for technical and vocational education, and for postsecondary education.[141] Our focus here is on K-12 public education and the system that enables the delivery of this essential public service. British Columbia's provincial government primarily exercises its constitutional jurisdiction over K-12 public education through the *School Act*.[142] Other statutory

[139] Thomas Fleming, "Provincial Initiatives to Restructure Canadian School Governance in the 1990s" online: (1997) No.11 Canadian Journal of Educational Administration and Policy

[140] *The Constitution Act, 1982, s. 93.*

[141] For administrative purposes, it is increasingly common for provincial governments to place early childhood learning and development under the umbrella of education.

[142] *School Act*, RSBC 1996, c 412.

instruments pertinent to public education include the *Teachers Act*[143] and the *Independent School Act.*[144]

In addition to statutory instruments, British Columbia's public education system is also a product of regulatory and policy instruments. Of particular significance is the 1989 *Statement of Education Policy Order* that was established through an order in council and remains an important source of policy guidance.[145] The 1989 *Statement of Education Policy Order* followed from the 1988 Royal Commission on Education, which is sometimes referred to as the Sullivan Report.

The complementary nature of legal and policy perspective is visible in the text of the School Act's preamble, which reflects the values articulated in the Sullivan Report and the *Statement of Education Policy Order*. Two portions of the preamble are indicative of the norms underlying the public education system and thus reviewed here. The very first paragraph of the *School Act* states that:

> It is the goal of a democratic society to ensure that all its members receive an education that enables them to become literate, personally fulfilled and publicly useful, thereby increasing the strength and contributions to the health and stability of that society[146].

The next paragraph then states that:

> The purpose of the British Columbia school system is to enable all learners to become literate, to develop their individual potential and to acquire the knowledge, skills and attitudes needed to contribute to a healthy, democratic and pluralistic society and a prosperous and sustainable economy[147].

---

[143] *Teachers Act*, SBC 2011, c 19.
[144] *Independent School Act*, RSBC 1996, c 216.
[145] Ministry of Education, *Annual Report* (2019), online: <https://www.bcbudget.gov.bc.ca/Annual_Reports/2018_2019/pdf/ministry/educ.pdf>. The *Statement of Education Policy Order* is referenced repeatedly in the Ministry of Education's most recent annual report.
[146] *School Act*.
[147] *School Act*.

Taken together, these two paragraphs in the preamble to the *School Act* point to the centrality of participation in democratic society and whole person education. The Act's prioritization of whole person education may be contrasted to Reich's notion of symbolic analysts, which had conceptualized education primarily as training for employment.

Consequently, the British Columbia provincial government has authority over K-12 public education. In turn, there is a foundational historical bargain in British Columbia between provincial oversight and local control, both of which underpin the structure of the public education system. This balancing act is enshrined in the *School Act*, which defines the powers and responsibilities of the province's Minister of Education and local school districts.

The School Act establishes the framework and the Minister of Education is the primary actor. Section 167 of the *School Act* requires the existence of a Ministry of Education and provides for the appointment of deputy minister and other employees required to conduct the business of the ministry.[148] Section 168 provides that the Minister of Education has charge of the maintenance and management of provincial public schools, must advise the Legislature on matters relating to education, and may make orders for the purpose of carrying out any of her statutory powers, duties, or functions.[149] The Minister of Education is therefore responsible for setting high level education policy. The following are specific areas in which the Minister exercises this responsibility and authority: establishing educational standards; monitoring and reporting on student performance; working with schools and communities to improve student and school performance; allocating funds for the education system; and, overseeing the governance of the system as a whole.[150] These five responsibilities can be described as the Minister's "Policy Tools" for shaping the public education system.

---

[148] *School Act, s 167.*

[149] *School Act, ss 168(1)-168(2).*

[150] Government of British Columbia, Education and Training, "What is Policy?", online: <https://www2.gov.bc.ca/gov/content/education-training/k-12/administration/legislation-policy/what-is-policy>.

In addition to the Policy Tools identified above, the Minister of Education has regulatory tools for guiding the operation of public education. The Minister's "Regulatory Tools" are its order-making power as well as its authority to make regulations and issue administrative directives.[151] The authority to issue administrative directives, in particular, creates a mechanism for mediating the relationship with local Boards of Education that can be used to discipline or encourage specific courses of action. For instance, under S. 168 (3) the Minister may issue an administrative directive to a Board of Education if the Minister believes that the Board is failing or has failed to meet its obligations under the Act, or it is in the public interest to do so.[152] Under S. 168(4) "The minister may, by order, issue an administrative directive to a board to enable the board to participate in or undertake a project in respect of the improvement of student performance or another matter specified by the minister.[153]

The second key actor in the public education system is the Board of Education in each school district. There are now sixty public school districts in British Columbia that are defined geographically. A useful lens through which to understand the activities and capacities of the school districts' Boards of Education is that of personnel, including employees and elected representatives from the community.

A school district's employees include district-level administrators, teachers and school support staff. Senior administrative roles include the Superintendent and Assistant / Associate Superintendent. A typical school district is unlikely to have more than one role focused on information technology.[154] The Superintendent's role, in turn, is similar to that of a Chief Executive Officer in a regulated public body. They are responsible for operational matters, such as supervision of schools, implementation of approved programs, evaluation of senior staff, overseeing of district budgets and reporting to the Board of Education.

The elected representatives from the community serve as members of the Board of Education and are referred to as Trustees. Under the *School Act* S. 65, the

[151] *School Act, ss 168(3)-168(4).*
[152] *School Act, s 168 (3).*
[153] *School Act, s 168(4).*
[154] Peter Holowka, "IT Leadership and Cloud Computing Adoption in Western Canadian K-12 School Districts".

Board of Education in a particular school district collectively constitutes a corporation.[155] S. 65(1) provides that:

> (1) The trustees elected or appointed under this Act for each school district and their successors in office constitute a board of education for the district and are continued as a corporation under the name of "The Board of Education of School District No. 5 (Southeast Kootenay)", or as the case may be.[156]

A significant part of the Board of Education's work is thus to allocate finite resources. In order to discharge this role, the Trustees must refine and develop the Board's corporate governance policies. In this respect, a Board of Education is akin to a board of directors. While a board of directors' reports to the company's shareholders, a Board of Education has significant financial reporting obligations to the Ministry of Education. Indeed, the Trustees oversee the school district's operating and capital budgets.

There are, however, at least three significant differences between a Board of Education and a corporate board. First, Trustees are ultimately responsible not only to the Ministry of Education but also to local voters through the ballot box. Second, a Board of Education has very limited opportunities to grow its resources. Third, a Board of Education has specific non-financial objectives. In this respect, s. 65 (1.1) provides that "A board is responsible for the improvement of student achievement in the school district."[157]

Consequently, a Board of Education and its Trustees must balance financial and non-financial responsibilities. Boards have a long list of objectives and inherently limited resources with which to achieve these objectives. This institutional context creates specific incentives for the decisions that Boards of Education will make about spending on information technology. A private business that is able to offer

---

[155] *School Act, s 65.*
[156] *School Act, s* 65(1).
[157] *School Act, s 65(1.1).*

a "free" solution is thus, at least according to a rational choice theory of decision-making, likely to receive an attentive audience from a Board of Education.

It is relevant to note that the *School Act* explicitly addresses the need to safeguard the personal information of students. Section 170 creates an obligation for a public body not to disclose personal information contained in a student record except for certain limited purposes.[158] Student record is defined under the *School Act* as "a record of information in written or electronic form pertaining to a student."[159] Historically, there was an expectation that a student record would be the public body's work product rather than a document created by a student.

The relevant s. 170 provides for disclosure pursuant to a "purpose authorized under the *Freedom of Information and Protection of Privacy Act*" and we thus return to the substance of these limited purposes in the more detailed discussion of disclosure in the next section.[160] It is sufficient to note that the expectation of a student's personal information not being disclosed outside the public education system is enshrined in the *School Act*.

By way of conclusion for this section, we can offer some broad observations about the institutional environment of the British Columbia public education system. The Minister of Education as part of the elected government exercises the province's jurisdiction over K-12 education. Over time, the Minister and the Ministry have created a province-wide system for executing this mandate. In turn, a significant part of the Ministry's work is simply to administer this system. The Minister also has broad oversight of the system and other actors in the system which it exercises through Policy Tools and Regulatory Tools. The other major actors in the system are the Board of Education in each of the province's sixty school districts. Under the system, administration of local operations is delegated to the school districts and associated responsibilities are discharged by the Boards of Education. The Boards of Education must work within the budget they are given and face ever increasing demands on these finite resources.

[158] *School Act*, s 170.
[159] *School Act, s 1.*
[160] *School Act, s* 170(1)(a).

4. PRIVACY RIGHTS AND RISKS

The *Freedom of Information and Protection of Privacy Act* ("FOIPPA" or "the Act") sets out the quasi-constitutional information privacy rights of individuals in respect of the public sector including the public school system.[161] British Columbia public bodies have statutory obligations under FOIPPA regarding the collection, use, disclosure, and storage of students' personal information including the obligation to exercise reasonable security.[162] This security obligation is not vitiated merely because a public body engages in contracting out. Rather, the law and various provincial policies create a set of requirements for public bodies that engage private service providers for data services such as cloud computing. In light of the available facts about the use of private internet platforms and software application in the public education system, the following three sections analyze:

- Students' Privacy Rights;
- Major Privacy Risks; and
- Security over Personal Information.

4.1 Individual' Privacy Rights

Individuals' information privacy rights are set out in FOIPPA. To deepen understanding of the specific provisions in FOIPPA on privacy rights, the following first examines FOIPPA's statutory purposes, its scope of application, and its definition of personal information.

FOIPPA sets out its dual purposes of protecting personal privacy and holding public bodies accountable to the public in s. 2:

> 2 (1) The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by

[161] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.
[162] *FOIPPA*

> (a) giving the public a right of access to records,
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
>
> (c) specifying limited exceptions to the rights of access,
>
> (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
>
> (e) providing for an independent review of decisions made under this Act.[163]

Sections 2(1)(a)-(e) sets out the primary duties public bodies must meet in order to fulfil the purpose of FOIPPA. Several of these duties are specifically focused on the protection of personal privacy, such as s. 2(1)(d), which deals with "preventing the unauthorized collection, use or disclosure of personal information by public bodies."[164]

It is helpful to review the broad scope of the term "public body." A public body is defined in FOIPPA Schedule 1 as including: a ministry of the government of British Columbia; or, a local public body.[165] Thus, the Ministry of Education is a public body. The definition of "local public body" includes an educational body, which is defined as "a board as defined in the *School Act*."[166] Because the definition of a board in the *School Act* includes a board of education, a board of education is an educational body and thus a local public body under FOIPPA.

FOIPPPA's scope of application is set out in FOIPPA s. 3. It provides that the Act applies to "records," defined in FOIPPA as: "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does

[163] *FOIPPA*, s. 2.
[164] *FOIPPA*, s. 2(d).
[165] *FOIPPA*, Schedule 1.
[166] *FOIPPA*, Schedule 1.

not include a computer program or any other mechanism that produces records."[167]

A "FOIPPA record" refers, therefore, to anything "on which information is recorded or stored" whether by graphic, electronic, mechanical or other means. Examples of a FOIPPA record are provided in the statutory definition and include "books, documents, maps, drawings, photographs, letters, vouchers, papers."[168] The statutory definition also indicates that a FOIPPA record "does not include a computer program"[169] which is instead, considered to be an example of a "mechanism that produces records."

The definition of a FOIPPA record therefore distinguishes between a thing on which information is recorded or stored on the one hand and the mechanism that produces aforesaid recording or storage on the other hand. The implications of this dichotomy are potentially wide ranging. For present purposes, however, it is reasonable to note that there is nothing in the statutory definition that would exclude the hard drive in a super computer of the type used in a cloud farm from being considered as a thing on which information is recorded or stored. In the case of cloud computing, there is, of course, more than a single hard drive and those hard drives are connected by certain mechanisms. Nevertheless, it is correct to state that information is being recorded or stored on a hard drive, i.e. in the form of a digital file, and that such a file may be considered to be a record under FOIPPA.

It is also helpful to review the broad scope of "personal information" as specifically applied under FOIPPA. As already noted, an expansive approach to the interpretation of personal information is favored by the Supreme Court of Canada. The Privacy Commissioner has provided specific guidance as to the meaning of the term personal information in FOIPPA, and notes that personal

[167] *FOIPPA*, Schedule 1.
[168] *FOIPPA*, Schedule 1.
[169] *FOIPPA*, Schedule 1.

information is, "recorded information about an identifiable individual."[170] This recorded information includes the following types of personal information:

> a) The individual's name, address or telephone number;
>
> b) The individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
>
> c) The individual's age, sex, sexual orientation, marital status or family status;
>
> d) An identifying number, symbol or other particular assigned to the individual;
>
> e) The individual's fingerprints, blood type or inheritable characteristics;
>
> f) Information about the individual's health care history, including a physical or mental disability;
>
> g) Information about the individual's educational, financial, criminal or employment history;
>
> h) Anyone else's opinions about the individual; and
>
> i) The individual's personal views or opinions, except if they are about someone else. [171]

Furthermore, the Privacy Commissioner writes that personal information is, "recorded information of any kind," so long as it is "about an identifiable individual."[172]

---

[170] Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document Data Services Contracts* (May 2003) at 2, online: Office of the Information & Privacy Commissioner <https://www.oipc.bc.ca/guidance-documents/1460>

[171] Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document Data Services Contracts*

[172] Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document Data Services Contracts.*

The Privacy Commissioner has reviewed the broad scope of personal information under FOIPPA in the context of the public education system for an applicant requesting access to electronic databases of 70 types of data elements, including each student's PEN, generated through the Ministry's Foundation Skills Assessment program.[173] In that matter, the Privacy Commissioner found that the PEN, as a unique number assigned to a student and used to link together different data elements about a student, is personal information. It further found that the additional 69 elements, with individual PENs attached, "are personal information in that they are about individual identifiable students, including how well they did in the FSA, whether they have a disability and so on." The Privacy Commissioner found that even if the PENs were removed or encrypted, there is a reasonable expectation that "all of the requested information, including PENs in encrypted or unencrypted form, is personal information."[174] Therefore, any eventual regulatory or judicial review of personal information collected, used, and disclosed through software applications will apply a broad definition of personal information.

The following subsections turn to specific privacy rights belonging to public school students in British Columbia under FOIPPA. These rights include the right to be protected against over- collection of their personal information; the right to be protected against improper use of their personal information; and the right to be protected against improper disclosure.

4.1.a Students' Right against Unauthorized Collection

The first example of the information privacy rights belonging to students in British Columbia's schools is the right not to have their personal information collected without lawful authority.

[173] Order F09-21 (2009) B.C.I.P.C.D. No. 27, online: <http://www.oipc.bc.ca/orders/2009/OrderF09-21.pdf>.
[174] Order F09-21 (2009) B.C.I.P.C.D. No. 27, at para 28.

Under FOIPPA, personal information may be collected only when permitted by law. FOIPPA s. 26 'Purpose for which personal information may be collected' sets out the specific, limited circumstances in which collection is permitted by law.[175]

Section 26(a)-(h) sets out a limited set of circumstances in which public bodies may collect personal information.[176] The most relevant of these subsections, s. 26(a)-(c) states that:

> **26** A public body may collect personal information only if
>
> (a) the collection of the information is expressly authorized under an Act,
>
> (b) the information is collected for the purposes of law enforcement,
>
> (c) the information relates directly to and is necessary for a program or activity of the public body.[177]

Therefore, the starting point in FOIPPA s. 26 is that personal information shall be collected by or for a public body "only if" – in the language of s. 26 – it is done pursuant to one of the listed circumstances. Furthermore, although it is not within the current scope to examine each of the circumstances set-out in s. 26 (a)-(h), it merits noting that the listed circumstances are specific. In other words, s. 26 (a)-(h) establishes a closed list: there is no "catch-all," "get out of jail free card," or "loophole" in the list in s. 26.[178]

These permitted purposes range from the very general, i.e. that the information is collected for the purposes of law enforcement,[179] to the relatively specific, i.e. the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to

[175] *FOIPPA*, s. 26.
[176] Order F07-10, 2007 CanLII 30395 (BCIPC) at para 29.
[177] *FOIPPA*, s. 26.
[178] FOIPPA s. 26(a)-(h)
[179] FOIPPA s. 26(b)

occur.[180] In the current matter, the most relevant FOIPPA permitted purpose is set out in s. 26(c), which has therefore been reproduced above.

FOIPPA s. 26(c) requires that any information collected by or for a public body both "relates directly to" and "is necessary for" a program or activity of that public body.[181] A preliminary consequence of this rule's structure is, thus, that the public body must have a specific "program" or "activity."

Furthermore, as the program or activity must be specific, it should be identified by the public body. In the current case of, e.g., G Suite for Education, therefore, each board of education must consider what the specific, identified "program" or "activity" for which the information is collected and necessary.

In addition to identifying the "program" or "activity" for which a service such as G Suite for Education may be used, the law set out in s. 26 (c) requires that it "relates directly to" and "is necessary for" that aforesaid "program" or "activity". Both are required: if even one of the requirements is not satisfied, then collection of students' personal information is not permitted under FOIPPA s. 26 (c).

The Privacy Commissioner has reviewed FOIPPA s. 26 on numerous occasions, and noted that s. 26 sets out a limited set of circumstances in which public bodies may collect personal information to carry out their mandates.[182]

The Privacy Commissioner has specifically considered s. 26(c) in respect of the public education system.[183] In an Order concerning the Board of Education of School District No. 75 (Mission), the Privacy Commissioner commented as follows:

> A relevant part of the interpretive context of s. 26(c) and FIPPA overall is the reality that governments need personal information to do their work. They cannot provide services, confer benefits or regulate conduct without our personal information. For this reason,

[180] FOIPPA s. 26(f)
[181] FOIPPA s. 26(c)
[182] British Columbia (Finance) (Re), 2019 BCIPC 41 (CanLII), <http://canlii.ca/t/j36kb>, retrieved on 2020-05-12, provides a reference to this general principle in Order F07-10, 2007 CanLII 30395 (BCIPC) at para 29.
[183] Order F07-10.

> citizens may be compelled by law to give up their personal information or will disclose it to receive services or benefits and one cannot ignore the power of the state in relation to personal information collection in interpreting what is meant by "necessary" in s. 26(c).[184]

The Privacy Commissioner emphasized that the word "necessary" should be interpreted in the context of the state's power to compel collection. Accordingly, the collection of personal information must be necessary for the relevant program or activity.

The British Columbia Supreme Court has also considered the scope of FOIPPA s. 26 (c). *In Collins v. City of Prince George*, the question arose as to whether or not the collection of certain personal information by the municipality could fall under FOIPPA s. 26 (c).[185] The court found that under s. 26 (c), "personal information collection must … be necessary for a program or activity of the public body." [186] It further found that enforcing a bylaw that was clearly intended to regulate the activities of entities other than the municipality did not qualify as necessary for a program under s. 26 (c).[187]

Accordingly, the necessity requirement is not *pro forma*. While there is a governmental power to compel, it must fall within the bounds of reasonableness and be related to the purpose. Thus, s. 26 (c) establishes a rigorous test that a school board, as a public body, must satisfy to engage in or have a service provider engage in the collection of students' personal information. Accordingly, there is a legal right in British Columbia not to be subject to over collection of personal information by or for a public body.

[184] Order F07-10, at para. 47.
[185] *Collins v. City of Prince George*, 2007 B.C.S.C. 1 (CanLII).
[186] *Collins v. City of Prince George*
[187] *Collins v. City of Prince George*

4.1.b Students' Right Against Unauthorized Use

The second information privacy right belonging to individuals in British Columbia's public schools is the right to be protected against improper use of personal information.

Section 32 of FOIPPA sets out how a public body shall use personal information.[188] As examined herein, the general principle is that personal information may be used only for the purpose for which it was collected.

FOIPPA s. 32 'Use of personal information' states that:

> **32** A public body must ensure that personal information in its custody or under its control is used only
>
> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
> (b) if the individual the information is about has identified the information and has consented, in the prescribed manner to the use, or
> (c) for a purpose for which that information may be disclosed to that public body under sections 33 to section 36.[189]

Section 32, therefore, sets out a basic rule and purposes for which personal information can be used by a public body. In this respect, it is similar in structure to s. 26 on the collection of personal information.

FOIPPA s. 32 requires a public body, such as a school board, to ensure that personal information in its custody or under its control is used only in accordance with the limited purposes set out in paragraphs (a) through (c). The word "only" indicates that use of personal information by or for a public body that is not consistent with one of the specific, limited purposes set out in paragraphs (a)

[188] FOIPPA, s. 32.
[189] FOIPPA, s. 32.

through (c) is not permitted. In turn, a public body is entitled to exercise its own discretion in determining whether it will rely on paragraph (a), (b), or (c). The following briefly reviews paragraphs (a) and (b), which may be invoked by a school board that chooses to provide students with access to private software applications.

Section 32 (a) requires that the use be only for the purpose that the personal information was obtained or a use consistent with that purpose. Each school board will have its own specific formulation of the FOIPPA 'permitted purpose' for which private software applications are permitted to obtain and thus use students' personal information. That formulation of the FOIPPA permitted purpose will establish a foundation for any future evaluation of whether specific types of use constitute a permitted purpose under s. 32(a).

FOIPPA s. 32(a) also allows use for a "consistent purpose". The term "consistent purpose" is defined in FOIPPA s. 34.[190] It creates a two-part test whereby the use under s.32(a) must both: a) have a reasonable and direct connection to the FOIPPA permitted purpose; and b) be necessary for a program or activity of the public body that uses the information.

The Privacy Commissioner has interpreted the term consistent purpose in s. 32 (a) as providing only a limited exception to use of personal information that is not for a FOIPPA permitted purpose.[191]

A second permitted purpose is contained in s. 32 (b), which allows a public body to rely on the individual's consent. Consent is implicitly invoked in some of the PIAs pertaining to Google's G Suite for Education.[192]

Use of personal information by or for a public body that is not within the narrow exceptions reviewed above is not permitted under FOIPPA.

---

[190] FOIPPA, s. 34.

[191] Vancouver Coastal Health Authority (Re), 2018 BCIPC 30 (CanLII), <http://canlii.ca/t/htj3t>,

[192] SD #72 - Campbell River, Privacy Impact Assessment for Google Suite for Education (GSFE) at 3, online: School District 72 Campbell River <https://www.sd72.bc.ca/studentsparents/GSFE/Documents/GSFE%20PIA%20%20for%20SD72%20FINAL%20DRAFT.pdf>.

4.1.c Students' Right Against Unauthorized Disclosure

The third core privacy right belonging to individuals in British Columbian public schools concerns the disclosure of their personal information.

The general principle is that public bodies have an obligation to only disclose personal information when applicable requirements are satisfied. Section 33 of FOIPPA sets out when a public body may disclose personal information. It states as follows:

> **33** A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3.[193]

Section 33, therefore, pertains to the disclosure of personal information that is either in the custody or under the control of a public body.[194] Furthermore, it authorizes disclosure only as permitted for specific, limited purposes in FOIPPA subsections 33.1 and 33.2 as introduced below.

Section 33.1 provides a set of permitted purposes for disclosure that is either inside or outside of Canada.[195] Section 33.2 provides a set of permitted purposes when disclosure is made inside of Canada.[196] The basic consequence is that disclosure within Canada is permitted in a wider set of circumstances than disclosure outside of Canada.

Both lists are technical and thus not reviewed comprehensively here. However, ss. 33.1(b) and 33.2(c) are relevant

---

[193] FOIPPA, s. 33.

[194] Public bodies frequently need to disclosure personal information to other parts of the provincial or federal public service in order to facilitate the administration of government. Associated issues were recently reviewed by the Privacy Commissioner, see: British Columbia (Finance) (Re), 2019 BCIPC 41 (CanLII), http://canlii.ca/t/j36kb.

[195] FOIPPA, s. 33.1

[196] FOIPPA, s. 33.2

Section 33.2(c) states in relevant part that:

> **33.2** A public body may disclose personal information referred to in section 33 inside Canada as follows:
>
> …
> (c) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;[197]

Accordingly, so long as disclosure is within Canada, a public body is entitled to disclose personal information to an "employee" in certain circumstances. Employee is a defined term in FOIPPA that includes, in relation to a public body, "a service provider."[198]

In the alternative, s. 33.1 sets out the limited circumstances in which disclosure may be made either inside or outside of Canada. Section 33.1 establishes the only basis on which disclosure may be made outside of Canada. It simply does not contain a provision that is equivalent to the relatively permissive approach found in s. 33.2, generally, and s. 33.2(c), in particular.

When a service provider is not located in Canada or intends to make disclosure outside of Canada, it must find a legislative door in s. 33.1 that the disclosure can pass through. Section 33.1(1)(b) allows for disclosure outside of Canada upon informed consent.[199] The door for disclosure in s. 33.1(1)(b) is, therefore, narrower and more restrictive than that in s. 33.2(c). Viewed on its face, the plain language of s. 33.1(1)(b) would suggest that each time disclosure is made outside of Canada the information must be identified and the impacted individual must consent. For this reason, some school boards have requested that students' guardian consent prior to disclosure of Stage 1 Information, i.e. allowing a local IT administrator to input the necessary biographical details for creating a G Suite for Education profile. However, it is less apparent that consideration has been given to the

[197] FOIPPA, s. 33.2(c).
[198] FOIPPA, s. 33.1(e.1).
[199] FOIPPA, s. 33.1(1)(b).

possibility of disclosure of Stages 2, 3, and 4 Information.[200] Issues of storage outside of Canada are examined further in part 4.2.iii of this report on disclosure risks.

In conclusion for this subsection, students in British Columbia's public education system have a legal right to be protected from improper disclosure of their personal information. More broadly, the quasi-constitutional nature of the privacy rights protected under FOIPPA is reflected in its status as fundamental legislation. Section 79 of FOIPPA provides that in the event of a conflict or inconsistency, the provision of FOIPPA prevails unless the other Act expressly provides otherwise.

The provisions of FOIPPA reviewed in this section establish specific, limited circumstances in which students' personal information may be collected, used, and disclosed by public bodies and their service providers. In the next section we examine risks associated with the available facts about collection, use, and disclosure of personal information through private software applications such as those provided through Google's G Suite for Education internet platform.

4.2 Major Privacy Risks

The preceding reviewed students' privacy rights. As examined further below in part 4.3, it is the responsibility of public bodies to safeguard these rights and the corresponding responsibilities under the School Act. According to the Ministry Guidelines prepared by the Privacy and Legislation Branch, Office of the Chief Information Officer in the Ministry of Citizens' Services, this means taking reasonable measures to manage privacy risks, where a privacy risk is understood as "something that could cause unauthorized collection, use or disclosure of personal information or result in any other contraventions of FOIPPA."[201] More

[200] Stages 2, 3, and 4 Information are described in part 2.3.b above.

[201] Ministry of Technology, Innovation and Citizens' Services, *Privacy Impact Assessment Guidelines* (2014), online: <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf >. See also, the current Ministry of Citizens' Services website, online <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments>.

concisely, a privacy risk may be described as any potential loss of control over personal information[202] In light of the broad and evolving definition of privacy risk, we turn now to consider the reasonably foreseeable privacy risks associated with the use of Google's G Suite for Education (the "Major Privacy Risks") under the basic categories of unauthorized collection, use, and disclosure.

4.2.a. Unauthorized Collection Risk

The first of the major privacy risks is the risk of unauthorized collection.

As examined above, the general rule is that a school board may collect students' personal information only when it has legal authority under s. 26. The FOIPPA permitted purposes, have been summarized in this manner by the OIPC, as:

- Collection expressly authorized by or under a legislative act;
- Collection for law enforcement purposes; and
- Collection related directly to and necessary for an operating program of the relevant public body.[203]

It is this third purpose that is most pertinent to collection that takes place when software applications are used in public school classrooms.

Consequently, a fundamental question is whether all of the personal information collected by software applications used in public school classrooms is directly related to and necessary for a program or activity of the relevant school board. The answer to this question cannot be decided in this report in part because it must be articulated by each school board in its own assessment. However, we do identify some of the relevant facts that will ultimately need to be considered.

Decision makers will need to consider the specific software application and how it is being used in a given school district. In this report, we have looked in greatest

[202]In recent years, this second definition has been recognized by the American Institute of Chartered Professional Accountants AICPA, *Privacy Risk Management*, online: <https://www.aicpa.org/interestareas/informationtechnology/resources/privacy-risk-management.html>.

[203] Office of the Information and Privacy Commissioner of British Columbia, *Guide to Access and Privacy Protection Under FIPPA* (2015), online: <https://www.oipc.bc.ca/guidance-documents/1466>.

detail at the use of Google's G Suite for Education ("GSFE"). The available facts about use of the software applications accessed through GSFE and published research about software industry business models both merit examination in some detail. Google's privacy policy is important particularly what it says about collection and how that policy has changed over time.

Under the schema for information flow introduced in part 2.3 above, Google's privacy policy sets out a broad scope of the collection of information, which may be in whole or in part personal information, by Google and its affiliates. Since 1999, Google's primary policy document on data collection has been revised more than thirty times.[204] Over that period, it has grown in length, technical detail, and overall complexity.

In the first version, Google stated that it collected only aggregated search activity, personal information provided by users, clickthrough information, and cookies.[205] In less technical terms, Google collected information that was provided directly or indirectly through an individual's interaction with its core service, i.e. internet search, as provided through the google.com website. The *New York Times* describes this document as "short and earnest, a quaint artifact of a different time in Silicon Valley, when Google offered 600 words to explain how it was collecting and using personal information."[206] Fast forward two decades later to the thirtieth version of Google's privacy policy, which was released in October 2019 with notable changes.

The 2019 version of Google's privacy policy contains a much longer list of personal data collected by the company – a complete list of the personal data collected Google would take up an entire page of this report. In brief, Google now collects "Things you create or provide to Google," "Your activity," "Apps, browsers, and device data," "Data from publicly accessible sources," "Data from

---

[204] In fact, Google maintains an archive of these changes. See, Google, *Privacy Policy*, online: <https://policies.google.com/privacy/archive?hl=en-US>.

[205] Google, *Privacy Policy*

[206] Charlie Warzel and Ash Ngu, "Google's 4,000-Word Privacy Policy Is a Secret History of the Internet" (July 2019), *New York Times* online: <https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html>.

partners," "Location data," and etcetera.[207] Not only is the list of data collected longer, but the ways in which data is collected have also expanded. Consider, for example, the category of "apps, browsers, and device data." In 1999, Google was collecting information that was shared through a specific web page in relation to a single application, i.e. internet search. In 2019, Google is collecting information that is collected by not only a wide range of applications but also Google's browser, Chrome, and the devices that are being used, such as tablets and smartphones.

By using Google's services, whether through a personal account or via credentials created within G Suite for Education, an individual submits an extensive amount of information. Information technology experts, such as Bruce Schneier, describe this is as a fundamental feature of the "freemium" business model through which Google provides, for example, software applications.[208]

The chains of data being collected by Google run parallel to the massive amounts of data now being produced. According to a 2017 report from a division of IBM focused on digital marketing, 90% percent of the world's data was created in the prior two years,[209] and according to the digital marketing consultancy DOMO, 2.5 quintillion bytes of data are created every day.[210] The proximate cause for this explosion of data is, simply, that more and more digital devices are being used by more and more people for longer and longer periods of time.

The distal cause for the explosion in production and collection of personal data has been described by Shoshana Zuboff – Professor Emerita at Harvard Business School – as surveillance capitalism. Professor Zuboff argues that companies such as Google

---

[207] Google, *Privacy Policy*.
[208] Bruce Schneier, *Data and Goliath: The hidden battles to collect your data and control your world*, (W.W. Norton & Company, 2015).
[209] IBM Marketing Cloud, "10 Key Marketing Trends For 2017" (2017), online: <https://totallygaming.com/eventblog/ice-live/ibm-marketing-experts-predict-10-key-marketing-trends-2017>.
[210] Domo, *Data Never Sleeps 5.0*, online: <https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1>.

> claim this private experience as free raw material for translation into behavioural data. Most data are hunted, captured and valued not for service improvement but rather for their rich predictive signals. These data flows lay the foundation for a lucrative new surveillance economy. First, data are extracted from private experience. Next, they are conveyed to computational factories called "machine intelligence," where they are fabricated into behavioural predictions. Finally, prediction products are sold to business customers in markets that trade exclusively in human futures, where companies compete on the quality of predictions: they sell certainty.[211]

Zuboff goes on to observe that, "[t]he competition to sell certainty produces economic imperatives: great predictions require data in volume and variety, economies of scale and scope."[212] This is, in a nutshell, the view that data is the new oil, which was introduced in the first section.[213]

In order to satisfy this demand for data, information technology companies, such as Google, are highly incentivized to distribute products that collect more extensive and more intimate data. The International Working Group on Data Protection in Telecommunications ("IWGDPT") has, for example, noted that data collected by software applications targeted at the education industry "may concern highly personal or sensitive information, including location, health, sleep patterns, social media activity."[214]

---

[211] Shoshana Zuboff "Toronto is surveillance capitalism's new frontier" *Toronto Life* (September 4, 2019), online: online: <https://torontolife.com/city/toronto-is-surveillance-capitalisms-new-frontier/>.

[212] Shoshana Zuboff "Toronto is surveillance capitalism's new frontier"

[213] Ariel Katz, *Data Libera?*

[214] International Working Group on Data Protection in Telecommunications, *Working Paper on E-Learning Platforms (61st Meeting, Washington D.C.)* (2017) at 10, online: <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf>. It should be noted however that the only reference is to an article in the *New York Times.* See, Khaliah Barnes, *Student Data Collection Is Out of Control* (September 2014), online: New York Times <http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data- collection-is-out-of-control>.

The IWGDPT further observes that, "physical educators, for example, might employ tracking and assessment tools that also monitor student's health-related habits and behavior outside of school."[215] Indeed,

> For the purpose of learning analytics, the scope of information that is demanded about the students may be even more excessive. Certain analytics tools employ information about social media activities, logs from online-gaming, online communities and physiological sensor data like eye-tracking or motion capture traces. Datasets of interest could include data about cognitive development, social learning, discourse progression, network interactions, learning paths through courses, competency completion and help-seeking behaviour.[216]

Based on the research conducted for this report, it is not currently possible to definitively exclude the risk that Google is collecting some of the types of datasets described in the above passage.

Furthermore, even if Google is not collecting any of the especially sensitive types of data-sets identified by the ICDPPC, there remains a risk that it might be collecting information through the software applications contained in GSFE that is not authorized under a FOIPPA permitted purpose. It is ultimately for the relevant public bodies to consider and assess whether the information collected by a service provider such as Google, as contemplated by the expansive terms of its 2019 privacy policy, are consistent with a FOIPPA permitted purpose.

In particular, the law on collection of personal information under FOIPPA s. 26 (c) demands a match between the factual circumstances of collection and the purpose invoked by the public body. School boards thus need to ask whether all of the information collected by Google is "directly related to" as well as "necessary for" the designated program or activity. Whether or not the collection of information is thought by Google to be 'necessary' for its own commercial

[215] International Working Group on Data Protection in Telecommunications, *Working Paper on E-Learning Platforms,* at 10.
[216] International Working Group on Data Protection in Telecommunications, *Working Paper on E-Learning Platforms,* at 11.

purposes does not factor into this analysis. Viewed from the perspective of British Columbia's public sector privacy law, a concern certainly arises about whether Google fully appreciates and is appropriately limiting its collection of students' personal information.

4.2.b Risk of Unauthorized Use

Following the risk of over-collection, major privacy risks associated with unauthorized use must also be considered.

Under FOIPPA, the basic rule is that a public body shall ensure that personal information – whether that information is in its custody or under its control – is used only for purposes consistent with the relevant subsection of s. 32. For the purposes of FOIPPA, data collected by a private software application remains legally under the control of the relevant public body even if it is in the custody of a service provider.[217] While Google does not assert an ownership interest in data gathered by G Suite for Education, questions do arise about how that data is used during the term of Google's custody. The risk of unauthorized use takes several specific forms, including unlawful processing, lack of transparency, lack of accountability, function creep, and a chilling effect. These are reviewed below.

The risk of unauthorized use of students' personal information can be understood by considering a prominent claim made by proponents of GSFE. The Greater Victoria School District (61) and Saanich School District (63) co-wrote a PIA for G Suite for Education in 2016. That PIA notes that "[a]s per the Google Apps for Education Terms of Service, Google does not serve ads nor use customer data for the purpose of advertising."[218] It is laudable that Google has foresworn serving ads to users associated with GSFE credentials. However, while advertising is a

[217] Google's "Terms of Use for G Suite for Education" do not provide that the data gathered by its software applications becomes the property of Google. See, Google for Education, *G Suite for Education Agreement*, online: <https://gsuite.google.com/terms/education_terms_japan.html>.

[218] Greater Victoria School District, *Privacy Impact Assessment for School District No. 61 (Greater Victoria) and School District No. 63 (Saanich)* (2018), online: <https://www.sd61.bc.ca/wp-content/uploads/sites/91/2018/09/GSuite-PIA-SD61_63.pdf>.

very well-known example of how Google has historically used users' data to generate revenue, it is far from being the only way in which data is monetized.

Certainly, the service of ads is a prominent aspect of using a standard Google account. Furthermore, it is generally understood that users of free Google credentials will have their personal data processed to be targeted by Google's advertising program, i.e. Google AdSense. It is tempting to prematurely conclude that AdSense is the only business line through which Google processes user data. However, AdSense is just one way in which Google can and does process personal information.[219]

The technological basis for Google's famous ability to serve up ads for users who are prepared to buy has evolved over time.[220] As of 2019, an increasingly important component of Google's leadership position is a technology called predictive analytics. Predictive analytics is the use of data, statistical algorithms and machine learning to identify the likelihood of future outcomes based on massive volumes of data. It entails a system that is closely related to but distinguishable from data mining, as data mining merely generates inferences from retrospective pattern analysis. Predictive analytics provides an assessment of what will happen in the future based on data about past activities that is both sufficiently accurate and inexpensive with the result that can efficiently replace human prediction.[221] Predictive analytics can be used in advertising but it is also being used in many other fields. Regardless of the economic sector, data remains a core input in predictive analytics. As a result, there is a basic commercial incentive to use the data gathered through G Suite for Education.

In this regard, review of the PIAs on G Suite for Education provide important insights about school boards' expectations as to how the data gathered by Google will or will not be used. Some British Columbian school boards recognize

[219] Douglas Edwards, *I'm feeling lucky: The confessions of Google employee number 59,* (Mariner Books, 2012).
[220] Douglas Edwards, *I'm feeling lucky: The confessions of Google employee number 59.*
[221] Ajay Agrawal, Joshua Gans, & Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence,* (Harvard Business Press, 2018).

that data gathered by Google's G Suite for Education will be used for improving Google's software.

For instance, the PIA prepared in Campbell River notes that "Google acknowledges that it tracks some browsing activity in connection with GSFE apps, but it does not attempt to identify individual users. Rather, it uses activity and access history to improve and maintain these products."[222] The reasonable implication is that the crude data sets and personal information obtained through G Suite for Education may be used to improve any of the software applications provided through this platform.

Use of data gathered through, for example, G Suite for Education's software applications raises questions about transparency. The OPC has written that meaningful transparency requires that information handling practices are conveyed in a way that is relevant to and actionable for end-users.[223] For the OPC, meaningful transparency requires consideration of the power dynamics and information asymmetries as between providers and end-users.[224] In turn, the OPC has queried whether it is possible to explain the intricacies and complexities of predictive analytics without resorting to excessive detail. It finds privacy law scholar Helen Nissenbaum's idea of a "transparency paradox" particularly useful in illustrating this problem. According to Nissenbaum:

> If a privacy policy finely details every flow, condition, qualification, and exception, it is unlikely to be understood, let alone read; however, summarizing information handling practices in a more simplistic style is no more helpful because it omits the important details that are likely going to make a difference for privacy.[225]

---

[222] School District 72 - Campbell River, *Privacy Impact Assessment for Google Suite for Education (GSFE)*, at 3.

[223] Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics: From Patterns to Predictions* (August 2012), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pa_201208/>.

[224] Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics*

[225] Helen Nissenbaum, "A Contextual Approach to Privacy Online" (2011) 140:4 Daedalus 32-48.

The OPC expresses concern that, therefore, "transparency is a difficult privacy principle to observe [in the context of predictive analytics]."[226]

Furthermore, the OPC has considered accountability and the importance thereof. For the OPC, accountability is a key governing principle for organizations that implement predictive analytics. Being an accountable organization is about more than simply having privacy policies or designating a chief privacy officer. Accountability is about having a business model that gives effect to all the privacy principles, and thus becoming an ethical enterprise. Fundamentally, ethics is about acting in consideration of the effects on others and in that way constantly assessing the privacy implications of conduct.

In a parallel vein, noted Canadian privacy and technology law scholar, the late Dr. Ian Kerr observed that increased use of predictive analytics raises concerns about accountability. Kerr asked whether the perception of increased efficiency, associated with predictive analytics, may lead to digital technologies replacing human judgement. He examined the legal system specifically and observes a shift from due process to pre-emption. He wrote that:

> Our concern is that big data's promise of increased efficiency, reliability, utility, profit, and pleasure might be seen as the justification for a fundamental jurisprudential shift from our current ex post facto system of penalties and punishments to ex ante preventative measures that are increasingly being adopted across various sectors of society. It is our contention that big data's predictive benefits belie an important insight historically represented in the presumption of innocence and associated privacy and due process values namely, that there is wisdom in setting boundaries around the kinds of assumptions that can and cannot be made about people.[227]

---

[226] Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics*.

[227] Ian Kerr & Jessica Earle, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy" (2013) 66 Stanford L Rev, online: <https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/>.

Kerr's focus was the legal system, but his concerns about digital technologies coming to monopolize decision making have broader implications. This decision-making can, in theory, relate to who can and cannot access domains that for most of the twentieth century have been seen as public goods, which would include both public law adjudication and public education. The promise of public education, in turn, has been that students are evaluated as individuals rather than as members of a group or data subjects that fall into a specific category.

In this regard, the IWGDPT has observed that, "the type and amount of data collected through e-learning platforms facilitates statistical analysis and profiling."[228] They have further remarked that:

> Providers of e-learning platforms or other companies use student data to make subjective assessments about, for example, student "sociability" and "enthusiasm". Intrinsic human biases in both data generation and system design may lead to unfair results for students, especially members of groups that have historically experienced discrimination. Inferences and judgments about students that are unrelated to academic performance may stigmatize them and limit educational opportunities.[229]

These observations lead to concern about potential "function creep" of the software applications provided by, for example, G Suite for Education.[230] The repercussions of function creep require one to imagine all possible results and account for these possibilities.

It also merits noting the potential chilling effect on students. For example, a recent study from Oxford University found empirical evidence that knowledge of government mass surveillance programs caused the public to be less likely to read

---

[228] International Working Group on Data Protection in Telecommunications, "Working Paper on E-Learning Platforms, 61st Meeting, 24-25 April 2017 (Washington D.C.)" at para. 12, online: <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf>.

[229] International Working Group on Data Protection in Telecommunications, "Working Paper on E-Learning Platforms, at 12.

[230] Bert-Jaap Koops, "The Concept of Function Creep" (forthcoming) 13:1 Law, Innovation and Technology.

articles about surveillance and other related topics online.[231] In parallel, students who are aware of constantly being monitored, via the various uses of their data reviewed above, may restrain expression of creativity and originality in the classroom. Students may feel compelled to adhere to traditional norms, or they may be deterred from articulating novel ideas out of concern that documentation of unorthodox ideas could be held against them in the future.

4.2.c Risk of Unauthorized Disclosure

Following the major privacy risks reviewed above, the risk of unauthorized disclosure also requires examination.

Under FOIPPA, the basic rule is that a public body shall ensure that personal information – whether that information is in its custody or under its control – is disclosed only when specific criteria are satisfied. This rule is, therefore, similar to the basic rules regarding collection and use; however, there is an additional legal detail that must be factored into any consideration of disclosure risks, i.e. the jurisdiction where the data is stored. Considering the specific example of Google and G Suite for Education, it appears highly probable that data will be stored outside of Canada. In particular, data will be stored in the United States. This raises a series of significant risks.

Section 30.1 of FOIPPA 'Storage and access must be in Canada' sets out requirements for storage of personal information in the custody of or under the control of a public body. Notwithstanding the title of this provision, exceptions to the general rule requiring storage in Canada are available. Reliance on an exception to store data outside of Canada does not eliminate the risks of unauthorized disclosure. FOIPPA s. 30.1 provides that:

> 30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:[232]

[231] Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 13:1 Berkeley Tech L.J.
[232] *FOIPPA*, s. 30.1

As a general rule, therefore, British Columbia's public bodies are expected to store personal information within Canada. British Columbia is one of only two Canadian provinces with this rule.[233] The exceptions to this general rule are intended to be limited.

For current purposes, FOIPPA s. 30.1(a) merits particular attention. It allows personal information to be stored outside Canada "if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction." Section 30.1(a) therefore requires that: each individual has identified the information, and has consented; and, that the consent has been given in the prescribed manner. These cumulative requirements must be fulfilled prior to the storage of said information outside of Canada. This is an exacting standard.

Materials reviewed for this report indicate that British Columbian school boards are aware that use of Google software applications involves data storage outside of Canada. Some school boards that are providing access to G Suite for Education have sent consent forms to the parents / guardians of participating students.

In the case of Google's G Suite for Education, for example, data collected by the relevant software applications is subject to being stored at any of the cloud farms in Google's global network. Table 4 lists the location of Google's cloud farms.

[233] During the Covid-19 related state of emergency, the rule has been temporarily suspended. *Ministerial Order No. M085* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085>; *Ministerial Order No. M180* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m180>; Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document FIPPA and online learning during the COVID-19* (April 2020), online: Office of the Information & Privacy Commissioner <https://www.oipc.bc.ca/guidance-documents/2402>

Table 4: Google Cloud Farm Locations[234]

Location (Present)
• Oregon, USA
• Iowa, USA
• Los Angeles, USA
• Las Vegas, USA
• Montréal, Canada
• Virginia, USA
• South Carolina, USA
• São Paulo, Brazil
• London, UK
• Frankfurt, Germany
• Eemshaven, Netherlands
• St Ghislain, Belgium
• Hamina, Finland
• Zürich, Switzerland
• Tokyo, Japan
• Osaka, Japan
• Jurong West, Singapore
• Hong Kong, China
• Changhua County, Taiwan
• Mumbai, India
• Sydney, Australia
• Seoul, Korea

[234] Google, *Cloud locations,* online: <https://cloud.google.com/about/locations>.

In general, data stored in Google's cloud resides in multiple cloud farms at various points in time. The laws of the relevant jurisdictions, i.e. where the data is stored, are likely to assert jurisdiction over that data. The closest of Google's cloud farms to British Columbia is in Oregon. Furthermore, while Google maintains a cloud farm in Montreal, that facility is new. Therefore, it is highly probable that data collected by G Suite for Education will be stored in the United States at some point in time. Accordingly, there is an expectation that this information will become subject to United States laws including the *Patriot Act* – a topic that has stimulated concern in the past and is examined in the final paragraphs of this subsection.

Questions certainly can and should be asked, and answered, about whether current practices for requesting consent are sufficient. The criteria articulated under s. 30.1(a) create an exacting standard whereby only informed consent is sufficient. This is an issue that was raised during public consultations for the current project. Parents noted a series of concerns, for example: the household is often inundated with a large volume of forms from the school;[235] the specific consent form for use of G Suite for Education provided only limited details about the information being collected and stored outside of Canada;[236] and, some school boards recognize that they must provide an alternative learning tool to students, but there is to date no evidence that such alternatives are actually being provided.[237]

For purposes of this subsection, however, the issue is not limited to whether informed consent has been obtained under s. 30.1. The issue is broader. Even if informed consent has been obtained, there continue to be risks of unauthorized disclosure, which are especially acute when data is stored outside of Canada. These risks are introduced below in terms of concerns about the *U.S.A. Patriot Act* ("*Patriot Act*").[238] In particular, *the Patriot Act* amended the *US Foreign*

[235] Parent of child in lower mainland school, public consultation held in Richmond B.C., Nov. 6, 2019.
[236] Parent of children in lower mainland schools, public consultation held in Richmond B.C., Nov. 6, 2019.
[237] Written submission of parent in Central Okanagan School District.
[238] *USA PATRIOT Act* (H.R. 3162).

Intelligence Surveillance Act[239] ("FISA") and expanded the circumstances under which the United States Federal Bureau of Investigation ("F.B.I.") can issue "national security letters".[240]

Prior to the *Patriot Act*, FISA already empowered United States authorities to gather intelligence on foreign agents in the United States and abroad. The Foreign Intelligence Surveillance Court ("FIS Court") issues secret orders under FISA allowing US authorities to gather information about individuals.

As noted above, once BC data is stored to Google's cloud, there is a significant probability that it will spend some time at a cloud farm in Oregon, and therefore become subject to United States laws. Accordingly, there is a risk that either a FISA order or a national security letter could be issued compelling disclosure of specific data, which illustrates the risk of unauthorized disclosure associated with cloud-based software applications.

4.3 Security over Personal Information

Preceding sub-sections examined the codification of students' quasi-constitutional information privacy rights as FOIPPA privacy rights and the major privacy risks associated with cloud-based software applications in the classroom. Concomitantly, British Columbia's public bodies have statutory obligations under FOIPPA pertaining in particular to the collection, use, and disclosure of personal information. These obligations crystalize in FOIPPA s. 30 'Protection of Personal Information' where they are described in terms of protecting the "security" of personal information.

This sub-section examines the threshold for compliance with FOIPPA s. 30. In particular, it looks at the how and the who of protecting the security of personal information under FOIPPA. In the case of private software applications being used in British Columbian classrooms, legitimate concerns arise as to whether reasonable measures are being taken to manage associated risks. Furthermore,

---

[239] Foreign Intelligence Surveillance Act of 1978, § 105(a)(3)(A), 50 U.S.C. § 1805(a)(3)(A) (2000) (amended 2001).

[240] This paragraph and the following paragraph were prepared with reference to *Privacy and the USA Patriot Act*.

in some parts of the province, questions are already being asked about whether the burden of managing risks associated with private software applications has been "outsourced" to households.

4.3.a Legal Compliance

British Columbian public bodies have statutory obligations regarding the security of personal information. The general principle established through FOIPPA is that public bodies must make reasonable security arrangements protecting personal information against certain risks.

The Supreme Court of British Columbia has noted that FOIPPA "[s]ection 30 requires the government, the public body, to make reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal."[241]

The text of s. 30 is as follows:

> Protection of personal information
>
> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.[242]

FOIPPA s. 30, therefore, has three components. First, it explicitly contemplates the risks of unauthorized collection, use, or disclosure. Second, it specifically applies to personal information that is either in the custody of or under the control of a public body. Third, it establishes a reasonableness standard.

The FOIPPA s. 30 obligation applies to personal information that is either in the custody of or under the control of a public body. A situation in which personal

---

[241] BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services), 2005 BCSC 446 (CanLII), <http://canlii.ca/t/1k1q4>, para 41.
[242] *FOIPPA*, s. 30.

information remains under the control of a public body while not being in its custody has historically arisen under contracting out schemes.[243]

Indeed, it is not uncommon for public bodies in British Columbia to contract out specific services to the private sector. Furthermore, contracting out is not, in itself, inconsistent with FOIPPA. For instance, FOIPPA s. 33(f) permits disclosure of personal information in the custody or under the control of a public body to an "employee" where the disclosure is necessary for the performance of the employee's duties. This needs to be read in conjunction with the expansive definition of "employee" that includes "a person retained under contract to perform services for the public body." [244] A "service provider" is defined under FOIPPA as "a person retained under a contract to perform services for a public body".[245] In this respect, when a public body enters into a contractual relationship to use a private cloud-computing service, the private provider becomes a service provider under FOIPPA.

The Privacy Commissioner has examined and provided guidance on relevant issues related to the contracting out of data services.[246] In that document, the OIPC identified three scenarios that are indicative of a public body having engaged a FOIPPA service provider. For example, it found that a public body was likely to have engaged a FOIPPA service provider where it has contracted out the processing or storage of information that includes personal information.[247]

Review of the available facts known about the use of, for example, Google's G Suite for Education is instructive. As introduced in Section 2.1, G Suite for Education is a cloud-computing service that includes Software as a Service (SaaS) functionalities. School boards that create G Suite for Education accounts are directly using that cloud computing service, and thereby gaining access to both the processing and storage of information in Google's cloud infrastructure, and the operation and management of computerized systems. As to whether the

[243] *Privacy and the USA Patriot Act*, at 110
[244] FOIPPA, Schedule 1.
[245] FOIPPA, Schedule 1.
[246] Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document Data Services Contracts*, at 2.
[247] Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document Data Services Contracts.*

relevant information includes personal information, the only tenable answer is "yes." For example, during the first stage in the flow of information, i.e. the creation of a user credential, there is no question that personal information is collected by G Suite for Education. Furthermore, personal information may also be generated during the second, third, and fourth stages, as described section 2.4.

The law is well-settled that a public public body cannot contract out of FOIPPA either directly or indirectly.[248] Personal information collected, used, or disclosed by a service provider under a contract with a public body remains in the control of the public body and the public body is accountable for the actions of the service provider in respect of that personal information. A public body, therefore, has an obligation to ensure that its service provider is in compliance with FOIPPA.

This brings us to the security standard that is required under FOIPPA. As noted above, the relevant provision explicitly requires public bodies to make reasonable security arrangements.

The Privacy Commissioner has recently reviewed the meaning of "reasonable security arrangements" in FOIPPA s. 30. It begins its analysis as follows:

> The reasonableness standard in s. 30 is measured on an objective basis and, while it does not require perfection, depending on the situation, it may signify a high level of rigor. To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards.[249]

In the case of G Suite for Education, we must therefore inquire what administrative, physical and technical safeguards have been adopted. The answer

[248] Order 04-19, [2004] B.C.I.P.C.D. No. 19; Order 00-47, [2000] B.C.I.P.C.D. No. 51 at paras. 10-45. Also see Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration), [2003] 1 F.C. 219 (C.A.) at para. 11; Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner) (1999), 180 D.L.R. (4th) 657 (Ont. C.A.); and Canada (Information Commissioner) v. Canada (Immigration and Refugee Board) (1997), 4 Admin L.R. (3d) 96 (F.C.T.D.) at para. 26.
[249] Investigation Report F13-02, [2013] B.C.I.P.C.D. No. 14.

would appear to be that, in the first instance, that certain safeguards have been adopted that are primarily administrative in nature. For instance, school boards have implemented administrative policies regarding use of G Suite for Education by students that may limit the collection of students' personal information.[250]

There is no publicly available information to suggest that school boards have directly adopted either physical or technical safeguards. Of course, we also need to consider the safeguards adopted by Google, to which we will return below.

In regard to the reasonableness of the administrative safeguards put in place by the school boards, the Privacy Commissioner's analysis of reasonableness under FOIPPA S. 30 introduces a baseline for assessing adequacy of specific safeguards:

> The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, the estimated costs of security, the relationship between the public body and the affected individuals and how valuable the information might be for someone intending to misuse it.[251]

It is important to note that the adequacy threshold ultimately depends on the sensitivity of the personal information and the relationship between the public body and the affected individuals.

In the current case, because the personal information is that of children, it should be considered to be sensitive or even highly sensitive. The relationship of trust between a school and its students must also be noted. As a provisional observation, the threshold for adequacy of any safeguards that have been adopted or will be adopted in the future may therefore be presumed to be high.

[250] School District #63, *G Suite for Education* (2016), online: <https://hub.sd63.bc.ca/mod/page/view.php?id=6482>.
[251] Investigation Report F13-02, [2013] B.C.I.P.C.D. No. 14.

Failure to implement reasonable security arrangements required under FOIPPA s. 30 have been examined in a recent report involving the Ministry of Education,[252] which highlights the highly sensitive nature of personal information belonging to children.

On 18 September 2015, the Privacy Commissioner was notified that the Ministry of Education was unable to locate a hard drive containing the personal information of more than 3 million students in British Columbia and the Yukon.[253] Several days later, the Privacy Commissioner initiated an investigation under FOIPPA s. 42(1)(a). In the investigation report, the Privacy Commissioner determined that this action was necessary due to the sensitivity of the information, the numbers of individuals affected by this breach, and the fact that most of the individuals affected were children or youth.[254] The investigation found that impacted personal information included not just name, gender, and date of birth, but also the individual's Personal Educational Number ("PEN") and whether the student was part of any of the following groups: cancer survivors, children in care, special needs students, children who withdrew from school, and post-secondary students receiving financial assistance. Furthermore, the Privacy Commissioner concluded that although there were sound privacy and security policies and directives in place at the Ministry, and employees were aware of these policies and directives, several Ministry employees engaged in a series of contraventions, whereby the hard drive containing personal information was moved offsite, for which the Ministry was accountable. The investigation report also notes that exclusively administrative safeguards are unlikely to be sufficient.[255]

In the case of software applications such as those accessed through Google's G Suite for Education, whether or not reasonable security arrangements are being made is far from clear. It is helpful to return to the schema of Software as a Service (SaaS). SaaS has both intermediary-users and end-users. Public bodies, such as

[252] 2016 BCIPC No. 5. FOIPPA authorizes government ministries to collect personal information, including sensitive personal information of children and youth, for the purposes of managing their programs and activities.
[253] 2016 BCIPC No. 5, at 6.
[254] 2016 BCIPC No. 5, at 7.
[255] 2016 BCIPC No. 5.

school boards, are the intermediary-users while students are the end-users. However, as noted previously and examined further below, these same public bodies have frequently elected not to negotiate an actual service agreement. Rather, they are accepting the terms and conditions of the foreign, trans-national corporations that market SaaS. The result is a tension between the corporation's privacy policy (as incorporated into the terms and conditions) and the end-users' privacy rights.

British Columbian public bodies have statutory obligations to protect the security of personal information, regardless of whether the personal information is in the public body's custody or under the public body's control. These obligations apply even when a public body elects to contract out. The following examines two legal mechanisms that have historically been used by public bodies to ensure that a FOIPPA service provider makes reasonable security arrangements.

4.3.b Selected Risk Management Tools

In light of public bodies' responsibility to make reasonable security arrangements to protect FOIPPA privacy rights, questions naturally arise about how the privacy risks associated with G Suite for Education should be managed. In fact, contracting out is sufficiently common that well established expectations have formed around certain best practices. Two risk management tools are especially pertinent: privacy impact assessments and service agreements. They are examined in the following.

Impact Assessments

It is now widely accepted that government initiatives involving personal information give rise to a need for a Privacy Impact Assessment. However, expectations around the exact form and substance of PIAs are case-specific. A helpful starting point is to recognize that a PIA is both a process and a document.

The PIA process is intended to evaluate and manage privacy impacts as well as ensure compliance with privacy protection rules and responsibilities. The provincial government describes a PIA as "an assessment tool used to evaluate privacy impacts, including compliance with the privacy protection responsibilities

under FOIPPA."[256] In British Columbia, "PIAs promote transparency and accountability, and contribute to continued public confidence in the way government manages personal information."[257] Accordingly, the PIA process should assist in determining whether government initiatives involving the use of personal information raise privacy risks. The PIA process should also measure, describe, and quantify any privacy risks. Furthermore, the process must be expected to generate solutions that either eliminate the privacy risks or mitigate them to an acceptable level. In this respect, the OPC has written that:

> PIAs are an early warning system, allowing institutions to identify and mitigate risks as early and as completely as possible. They are a key tool for decision-makers, enabling them to deal with issues internally and proactively rather than waiting for complaints, external intervention or bad press.
>
> An effective PIA can help build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices.
>
> A PIA report documents the PIA process. The real value comes from the analysis that occurs as part of the process of working through the PIA questions.[258]

Under FOIPPA, there is no mandatory format for the PIA document. The provincial government does however make available six types of templates for PIAs

- General PIA for Ministries;
- General PIA for Other Public Bodies;
- Initiative Update PIA;
- Corporate PIAs;

---

[256] OXD, *Navigating the PIA Process in the BC Provincial Government*, online: <https://oxd.com/insights/navigating-pia-process-provincial-government/>.
[257] OXD, *Navigating the PIA Process in the BC Provincial Government.*
[258] Office of the Privacy Commissioner of Canada, *Expectations: OPC's Guide to the Privacy Impact Assessment Process* (2020), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.

- Legislation PIAs; and
- Regulation PIAs.

The General PIA for Other Public Bodies template has been used in part or in whole by some school boards that are known to be using, for example, Google's G Suite for Education.[259] However, certain concerns persist. First, there is a concern that a PIA template is susceptible to becoming an exercise in ticking boxes, or the formulaic completion of pre-set questionnaires. Second, as noted above in section 1 of this report, by no means all software applications used in British Columbian classrooms are subject to school board-level oversight. Rather, it is still very common for individual schools and even teachers to make decisions regarding the use of specific software applications that have privacy impacts.

From the perspective of fundamental legal principles, and in respect of the first concern noted above, it is instructive to return to the Supreme Court of Canada jurisprudence (exposited in s. 3.2 above) on informational privacy. The Supreme Court of Canada has recognized on numerous occasions that the *Privacy Act* has quasi-constitutional status and privacy interests are worthy of protection under the *Charter.*[260] The logical consequence of this approach is to consider that privacy risks of a government initiative should be measured in the context of their potential impact on democratic society and civil liberties. It is exactly this approach that has been followed by the OPC in its review of PIAs. The OPC exercises a review function over PIAs not accorded to British Columbia's Privacy Commissioner.

The federal Privacy Commissioner has publicly stated its intention of asking the authors of PIAs to answer questions based on constitutional law principles for weighing reasonable limitations on rights and freedoms in a free and democratic

[259] See, for example, Nanaimo Ladysmith School District, *Privacy Impact Assessment for School District No. 68*, online: <https://www.sd68.bc.ca/wp-content/uploads/GSFE_PIA_NLPS.pdf>.

[260] Dagg v. Canada (Minister of Finance); Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police) [2003] 1 S.C.R. 66; Lavigne v. Canada (Office of the Commissioner of Official Languages) [2002] 2 S.C.R. 773; and H.J. Heinz Co. of Canada v. Canada (Attorney General) [2006] 1 S.C.R. 441.

society.[261] The relevant four questions, which are based on the leading *Charter* case of *R. v. Oakes*, are:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy-invasive way of achieving the same end?[262]

These questions point to the need for PIA documents to contain a substantive analysis, rather than merely "ticking boxes." In turn, this type of substantive analysis would need to carefully balance the legitimate interests of various stakeholders. In the case of PIAs on Google's G Suite for Education, for example, this substantive analysis is regrettably difficult to identify.[263]

Service Agreements

Historically, contracting out has often involved a public body transferring custody over records containing personal information to a service provider pursuant to a service provider agreement ("SPA"). In the case of software applications, relevant public bodies have not expressly transferred records to a service provider; however, software application providers directly collect personal information from students. The result is that a service provider may have custody of personal information over which public bodies have security obligations. Notwithstanding these security obligations, public bodies have declined to negotiate SPAs let alone specific terms related to protecting privacy with the operators of private software applications.

---

[261] Office of the Privacy Commissioner of Canada, *Expectations: OPC's Guide to the Privacy Impact Assessment Process.*

[262] R. v. Oakes [1986] 1 S.C.R. 103.

[263] In addition to PIAs, we also note the increasingly common practice of conducting a Security Threat and Risk Assessment (STRA). An STRA assesses and reports on security risks. For new or significantly modified information systems within core government, STRAs are now established best practice in British Columbia. Public bodies external to core government are increasingly encouraged to complete an STRA in the relevant circumstances.

Following adoption of the recommendations of the Privacy Commissioner in the *Privacy and the USA Patriot Act* report provincial Ministries have been required as a matter of policy to complete and attach a privacy protection schedule for all contracts with a service provider that involve personal information owned or controlled by government.[264] The privacy protection schedule is intended to ensure that the high privacy standards set by FOIPPA are maintained for personal information in the custody of service providers. The privacy protection schedule's requirements for collection are illustrative:

> Collection of personal information
>
> 1. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
> 2. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
> 3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
>
>   (a) the purpose for collecting it;
>   (b) the legal authority for collecting it; and
>   (c) the title, business address and business telephone number of the person designated by the Province to

[264] *Privacy Protection Schedule is available online at the Government of British Columbia's web page,* https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule

> answer questions about the Contractor's collection of personal information.[265]

The above concisely sets out the expectation on the service provider to prevent excessive collection. Therefore, negotiation of an SPA with Google and inclusion of the privacy protection schedule therein would be one possible mechanism for managing the excessive collection risk in the current case.[266]

The *Privacy and the USA Patriot Act* report also had significant impact in Alberta. Alberta's Office of the Information and Privacy Commissioner generated its own report entitled "Public-sector Outsourcing and Risks to Privacy." In that report, Alberta's Information and Privacy Commissioner reviewed the changes in contracts between British Columbia's public bodies and outsourcing service providers following the Health Benefits Case. The Commissioner found that certain new features were appearing in such contracts, which we believe ought to be considered in inclusion in BC's privacy protection schedule:

- Requirements for segregated data access;
- Requirements to keep individual user logs;
- More use of non-disclosure agreements (between individual service provider employees and the public body, between employees of a sub-contractor and the service provider, and between employees of the sub-contractor and the public body);
- Annual oath requirements for service provider and sub-contractor employees;
- Restrictions on access of foreign- based employees to personal information, where these employees work on transition and transformation activities;

---

[265] *Privacy Protection Schedule*, online: <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule>.

[266] In the case of private software applications such as those accessed through Google's G Suite for Education the public bodies that are directly involved are school boards not the Ministry. Nevertheless, the underlying obligation in FOIPPA, i.e. to make reasonable security arrangements, applies.

- Limitations on data access generally, including data remote access;
- Corporate internal limitations on data access, cutting off extra-provincial access;
- Alarm notification facilities to alert the public body to copying or unusual access activity;
- Prohibitions on service provider staff outbound Web and e-mail access;
- Restrictions on data portability hardware to only designated personnel;
- Dedicated service provider privacy officers to monitor compliance; and
- Financial penalties in contract in the event of disclosure or privacy breaches.[267]

In the case of classroom software applications, the inclusion of contractual provisions that are responsive to and attempt to mitigate privacy risks is a best practice that merits further consideration.

Ideally, the forms of contractual risk management reviewed in this section would be utilized in concert with another best practice meriting further consideration: a PIA that documents substantive analysis and management of privacy risks. Unfortunately, questions persist about whether the relevant public bodies have pro-actively managed privacy risks associated with private software applications.

[267] Office of the Information and Privacy Commissioner for Alberta, *Public-sector Outsourcing and Risks to Privacy* (2006), online: < http://www.assembly.ab.ca/lao/library/egovdocs/2006/alipc/153159.pdf>.

5. BEST PRACTICES FROM OTHER JURISDICTIONS

Internet platforms offer education authorities a financially inexpensive mechanism for accessing software applications. Alongside the advantages associated with introducing students to the internet, increasing use of software applications in the classroom also opens the door to a range of ethical, policy, and legal concerns associated with students' privacy. Sections three and four examined the overarching privacy law principles and core rules protecting students in British Columbia's schools. We have seen that the current approach to these platforms does not necessarily represent a fair distribution of privacy risks and the associated risk management burden. In this section we ask: how can and should the relevant public bodies improve their practices in order to more comprehensively manage risks arising from the cross-border collection, use, and disclosure of personal information by such service providers?

To answer this question we look at approaches taken in other jurisdictions. In the "borderless" world created by the internet, and intensified by the wide-spread adoption of cloud computing, the effectiveness of privacy protections imposed by British Columbian or Canadian law is limited. The effectiveness of any new powers granted to and enforcement capacity exercised by the Privacy Commissioner in British Columbia is inextricably interdependent with events in foreign jurisdictions. In *The Governance of Privacy*, University of Victoria political scientist Colin J. Bennett analyzed exactly the problem of whether interdependence produced a "race to the top" or "a race to the bottom". Bennett found that the result up until the early 2000s was in fact something less unidirectional and more complex. He found that complexity was characterized by a "toolbox" of policy measures available to governments. The four types of "tools" in this toolbox were: transnational negotiations, domestic privacy authorities, self-regulation by firms, and technical.[268] Bennett's analysis was influential amongst political scientists and provides a helpful starting point on cross-border privacy issues. It is the initiatives of domestic regulators and

[268] Colin J Bennett and Charles D Raab, *The governance of privacy: Policy instruments in global perspective* (Routledge, 2017).

articulation of transnational norms that merit closest attention. The following sections do exactly just that.

5.1 Privacy Authorities

A limited number of domestic privacy regulators have directly addressed the use of software applications in public school classrooms.

Spanish authorities are understood to have published a report about the results of an of an *ex-officio* inspection on education-related cloud services. According to a summary made available by the International Conference of Data Protection and Privacy Commissioners, the Spanish report includes a set of recommendations for interested stakeholders that covers issues such as security, data location, contractual clauses, controller-processor relationship, information to users, cloud services, mobile apps and etcetera.[269] However, to date the report is only available in Spanish. It has, thus not been reviewed for the purposes of this report and is not introduced further.

The German National Conference of Data Protection Commissioners also recently published a report about issues associated with education-related cloud services. [270] The relevant report is, however, only available in German and has thus not been substantively reviewed by the author.

Recent the Information and Privacy Commissioner of Ontario ("IPC") has taken preliminary steps to address the use of software applications in public school classrooms. In January 2019, the IPC published *A Guide to Privacy and Access to Information in Ontario Schools* ("IPC guide").[271] The IPC guide introduces

[269] Agencia Espanola Proteccion Datos, *Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos* (2020), online: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Inspeccion_cloud_edu cacion.pdf> (in Spanish).

[270] German National Conference of Data Protection Commissioners, *A Guidebook From the Data Protection Supervisory Authority for Online Learning Platforms in School Classrooms*, copy of document on file with author.

[271] Information and Privacy Commissioner of Ontario, *A Guide to Privacy and Access to Information in Ontario Schools* (2019), online: < https://www.ipc.on.ca/wp-content/uploads/2019/01/guide-to-privacy-access-in-ont-schools.pdf>.

Ontario's privacy legislation pertaining to students' personal information in public school classrooms.

The IPC guide covers the types of personal information that can be collected by school boards as well as when, how, to whom, and to what extent such information may be collected, used, disclosed, retained or corrected. More specifically, the IPC guide reviews the rights and obligations of school board officials regarding students' personal information in the following seven topics: collecting personal information; using and disclosing personal information; consent to collect, use and disclose personal information; safeguarding and retaining information; access to information; correction of personal information; special topics. Of particular note, under special topics, the IPC guide addresses the topic of privacy in the networked classroom and the use of online educational services. [272]

The IPC guide also acknowledges that Ontario teachers often use online educational tools and services in their classrooms, sometimes without the knowledge or approval of school administrators and school boards. The IPC guide notes that "[w]hile these services may be innovative, readily accessible, and available at little or no cost, their use may pose privacy risks to students and their families."[273] Under the applicable statute in Ontario, the IPC guide further notes that school boards are accountable for online educational services used in the classroom. Accordingly, school boards "must ensure that these services do not improperly collect, use or disclose students' personal information". The IPC guide then identifies three examples of risks associated with internet platforms, i.e. improper collection, unauthorized use, and unauthorized disclosure of students' personal information.[274]

---

[272] Information and Privacy Commissioner of Ontario, *A Guide to Privacy and Access to Information in Ontario Schools*

[273] Information and Privacy Commissioner of Ontario, *A Guide to Privacy and Access to Information in Ontario Schools*

[274] Information and Privacy Commissioner of Ontario, *A Guide to Privacy and Access to Information in Ontario Schools*

Given these privacy risks, the IPC guide then recommends that schools and school boards using online educational services take the following steps prior to using internet platforms in the classroom:

- Develop and implement policies to evaluate, approve and support the use of online educational services for use in the classroom;
- Consider carrying out a privacy impact assessment and working with other educational stakeholders prior to using any particular online educational service;
- Take precautions before accepting so-called "take-it-or-leave-it" terms and conditions;
- Provide educators with a list of online education services which are approved for use in the classroom;
- Provide privacy and security training and ongoing support for teachers and staff;
- Notify students and parents about the personal information that may be handled by the online services and the reasons for handling it;
- Allow for students or parents to opt out of online educational services that collect, use, retain or disclose personal data;
- Provide other ways to deliver the same educational services;
- Set and enforce retention periods for accounts and different categories of personal data;
- Routinely purge logs of interactions between students, parents and educators. (collectively, "IPC guide recommendations")

The IPC guide's recommendations are considered further in the conclusion of this report.

5.2 Transnational Networks

In addition to the initiatives taken by domestic authorities, several transnational networks have considered privacy issues related to internet platforms and software applications in schools. For ease of reference, we have grouped these materials in two broad categories: working group reports; and, non-binding resolutions. Sections 5.2.i through 5.2.iii thus review the three transnational

networks that have, as of January 2020, generated working group reports on internet platforms in public school classrooms.

5.2.i International Working Group on Data Protection in Telecommunications: Working Paper on E-Learning Platforms

One example of such a transnational network is the International Working Group on Data Protection in Telecommunications ("IWGDPT"). The IWGDPT was established in 1983 and its members include national data protection authorities and representatives from the private sector and non-governmental organizations.[275] Its secretariat is provided by the data protection authority of Berlin.[276] In recent years, IWGDPT has worked on various projects pertaining to data protection and privacy.[277]

The IWGDPT's Working Paper on E-Learning Platforms begins by noting that "[d]espite the privacy challenges that surround the use of e-learning platforms, it is possible to use these types of platforms without infringing key privacy principles."[278] The Working Paper then recommends to education authorities that they:

- Should engage technology providers that offer sufficient guarantees to ensure that the privacy and data protection rights of students are adequately protected;
- Should conduct a privacy impact assessment and a risk analysis prior to use;
- Should implement the necessary technical and organizational measures according to the analysis before and while using the outsourced services (these measures should be continuously monitored and improved);

[275] European Data Protection Supervisor, *Glossary*, online: <https://edps.europa.eu/data-protection/data-protection/glossary/b_en>.
[276] European Data Protection Supervisor, *Glossary*.
[277] European Data Protection Supervisor, *Glossary*.
[278] International Working Group on Data Protection in Telecommunications, *Working Paper on E-Learning Platforms*

- Should avoid "lock-in" situations where personal data of students is tied in a black-box processing platform with poor transparency and control;
- Must obtain parental consent whenever necessary; and
- Must ensure that they retain full control over any determinations or evaluations made about students, especially in case of automated decision-making (collectively, the "Working Paper recommendations").[279]

The Working Paper's recommendations are considered further in the conclusion to this report.

5.2.ii GPEN Sweep Report

The Global Privacy Enforcement Network (GPEN) was established in 2010 with the aim of fostering cross-border cooperation among privacy regulators. It is composed of over 60 privacy enforcement authorities from 39 states. Each spring, as part of an annual information exchange activity, certain GPEN members conduct a review of privacy risks associated with a specific type of website or application report back to the entire GPEN network. This activity is referred to as a "SWEEP."

In 2017, the theme of the GPEN SWEEP was user control over personal information and the Ontario IPC participated as a reviewing member.[280] On the basis of consultation with educators and school board staff about internet-based services being used in schools, the IPC reviewed more than twenty websites. The goal was to understand the transparency practices of these online educational services, which was defined in terms of the following questions: whether the website informs educators and students how they collect, use and disclose personal information; and how much effective control educators and students can exercise over their information that is collected, used and disclosed by the service

[279]International Working Group on Data Protection in Telecommunications, *Working Paper on E-Learning Platforms.* The Working Paper offers recommendations that are addressed to both education authorities and technology providers.

[280] Information and Privacy Commissioner of Ontario, *2017 GPEN Sweep Report: Online Educational Services* (October 2017) online: <https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt.pdf>.

provider and third parties.[281] The IPC ultimately arrived at a series of best practice recommendations for teachers, which are summarized here:

- Teachers should consult with the school board, principal and/or administrators before selecting and using an online education service;
- Teachers should read the privacy policies and terms of service to understand what personal information about students may be collected, used and disclosed by the online educational service;
- Teachers should minimize the identifiability of students and the collection of their personal information by the online educational service, where feasible;
- Teachers should seek the involvement and express consent of parents and guardians, where appropriate; and
- Teachers should provide timely and ongoing guidance to students on appropriate uses of online educational services (collectively, "GPEN Recommendations").[282]

The GPEN recommendations are considered further in the conclusion to this report.

5.2.iii International Conference of Data Protection and Privacy Commissioners Digital Education Working Group Reports

The third transnational network is the International Conference of Data Protection and Privacy Commissioners ("ICDPPC").[283] In October 2019, the ICDPPC re-branded itself as the Global Privacy Assembly. The old nomenclature is used in this report for the sake of consistency, i.e. for the titles of documents issued prior to October 2019.

---

[281] Information and Privacy Commissioner of Ontario, *2017 GPEN Sweep Report: Online Educational Services*, at 2.

[282] Information and Privacy Commissioner of Ontario, *2017 GPEN Sweep Report: Online Educational Services*, at 7-8.

[283] Global Privacy Assembly, *Digital Education Working Group Report on Survey*, Online: <https://icdppc.org/wp-content/uploads/2017/12/DEWG-Research-Paper-Canada- eplatforms_Sept-2017.pdf>.

The ICDPPC is a leading global forum for domestic authorities with a data protection and privacy mandate. It aims to provide international leadership in light of the collective action problem identified in the introduction to this section. As of January 2020, there are more than 130 accredited members.[284] Members convene annually to participate in working groups and committees devoted to thematic issues and develop public resolutions and reports. The ICDPPC's Digital Education Working Group ("DEWG") established the technical foundation for the ICDPPC's resolution on e-learning platforms, which is reviewed in the following subsection. The DEWG's initiatives leading up to the ICDPPC resolution are reviewed here.

The ICDPPC DEWG was established in 2013 under the leadership of French data protection authority Commission nationale de l'informatiques et des libertés.[285] After 28 data protection authorities joined the DEWG in the first quarter of 2014, three priority actions were identified, including establishing an international competency framework for privacy education.[286] The DEWG's 2017 annual report identified for the first time the emerging issue of "widespread use on the part of the education community of eLearning platforms, online services and applications dedicated to the education community with regards to privacy issues."[287]

Of particular note, the DEWG's 2017 annual report observed that:

> Many of e-Learning platforms and educational services facilitate collaborative learning and communication, but in doing so, also

[284] To be accepted into the Conference, members must be the highest data protection or privacy enforcement body in their state, with an "appropriate range of legal powers" and "autonomy and independence." See, Global Privacy Assembly, *History of the Assembly,* online: <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.
[285] International Conference of Data Protection and Privacy Commissioners resolution *"Resolution on Digital Education for All" at the 31st International Conference of Data Protection and Privacy Commissioners in September 2013*
[286] Global Privacy Assembly, 2014-2015 Action Plan Program of the International Working Group on Digital Education (2014), online: <http://globalprivacyassembly.org/wp-content/uploads/2015/02/Digital-Education-2014-2015-Action-Plan-EN1.pdf>. Under Action 2, the French data protection authority sent a brief questionnaire (cf. Appendix 1) to all ICDPPC Members and subsequently the DEWG issued a report on the basis of the answers received.
[287] Global Privacy Assembly, *Report of the International Working Group on Digital Education* (2017) at 6, online: <http://globalprivacyassembly.org/wp-content/uploads/2015/02/Digital-Education-Working-Group-Report-1.pdf>.

> collect vast amounts of sensitive personal information about students, including behaviours, attitudes and students' personal data. But, are students' personal information appropriately protected?[288]

In 2017, there was also increased involvement in the DEWG by Canada's federal OPC. Acting on behalf of the DEWG, Canada's OPC circulated a questionnaire to ICDPCC members in July 2017.[289] The questionnaire aimed at canvassing members' opinions and experiences regarding use of what it referred to as "e-learning platforms" by educators and students. The results of the questionnaire were reviewed by Canada's OPC and summarized in a report that was circulated back to the entire ICDPCC membership in September 2017.[290]

In 2018, the DEWG further considered proposed recommendations regarding the practices of online platforms aimed at the education sector with regard to data protection and privacy issues. It prepared draft text of a resolution that was, at this point in time, conceptualized as being aimed at educators and service-providers. The draft resolution contained a series of recommendations seeking to allow digital services to be used in schools whilst guaranteeing the full and effective integration of data protection and privacy rules applicable to public schools.[291] The text of the resolution is reviewed in section 5.3.

In June of 2019, following the resolution's approval by the ICDPCC members, the French data protection authority and Canada's OPC distributed a questionnaire to all DEWG members to collect information about the impact of the promotion of the resolution. The results of the questionnaire have not at the time of writing been made public. It may be that they will be included when the 2020 report of the DEWG is published later this year. The DEWG notes an intention to use the results of the questionnaire to "take stock of the various types of Codes of Practice and/or Guidelines based on or in relation to the present resolution specifically

---

[288] Global Privacy Assembly, *Report of the International Working Group on Digital Education* (2017) at 6, online: <http://globalprivacyassembly.org/wp-content/uploads/2015/02/Digital-Education-Working-Group-Report-1.pdf>.
[289] Global Privacy Assembly, *Report of the International Working Group on Digital Education* (2017)
[290] Global Privacy Assembly, *Report of the International Working Group on Digital Education* (2017)
[291] Global Privacy Assembly, *Report of the International Working Group on Digital Education* (2017)

adapted to the local context and laws to help protecting children's data in an appropriate way."[292] As examined further in the conclusion to this report, the DEWG is one institutional forum through which authorities in British Columbia, i.e. the Privacy Commissioner, may exchange best practices regarding online platforms and software application in schools.

5.3 ICDPPC Resolution

The ICDPPC 40th International Conference, in 2018, issued six resolutions, including the ICDPPC's *Resolution on E-Learning Platforms*.[293] Resolutions of the ICDPPC are non-binding, but this soft-law instrument is nonetheless relevant to our report. It provides a helpful indication of the direction in which transnational norms are evolving.

The ICDPPC's *Resolution on E-Learning Platforms* contains 24 recommendations in total. These recommendations are variously addressed to educational authorities, technology providers, and data protection authorities. The notion of a data protection authority is broadly equivalent to the provincial and federal privacy commissioners that are established under Canadian law. For current purposes, the recommendations for public bodies are particularly relevant. We will also review the recommendations for data protection authorities.

Under the ICDPPC *Resolution on E-Learning Platforms*, six recommendations are addressed directly to educational authorities.[294] These are to:

1. Ensure they have appropriate authority and expertise to engage the services of technology providers;

[292] International Conference of Data Protection and Privacy Commissioners, *Report of the International Working Group on Digital Education* (2019), online: <http://globalprivacyassembly.org/wp-content/uploads/2019/11/2018-2019-Activity-Report-V-final_DEWG_working-group-on-digital-education.EN_.August-2019.pdf>.
[293] Global Privacy Assembly, *Resolution on E-Learning Platforms* (2018), online: <http://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf>.
[294] Global Privacy Assembly, *Resolution on E-Learning Platforms*

2. Develop policies and procedures to evaluate, approve and support the use of internet platforms including data protection/privacy impact assessments;
3. Provide training and on-going support for educators;
4. Work with other educational authorities and, in cooperation with local data protection authorities, to agree on common standards;
5. Where required or appropriate, seek valid, informed and meaningful consent from individuals; and
6. Consistent with domestic law, implement a policy for individuals who access the e- learning platform with their personal electronic devices. This policy should clarify appropriate uses of the e-learning platform and any consequences of using a personal device – especially when installing software or mobile applications (collectively, the "ICDPPC recommendations").[295]

On the first point, the ICDPPC anticipates that there should be clear allocation of roles and responsibilities between educators, administrators and other relevant educational authorities. This establishes legal authority and accountability when contracting with technology providers. The representative(s) of private service providers should have a clear understanding of applicable privacy laws so as to include such laws in the terms and provisions of service agreements.

On the second point, the policies anticipated by the ICDPPC should promote individual control over personal data, clarify the roles and responsibilities among the various actors involved in e-learning platforms, mitigate risks, and promote accountability.

On the third point, the ICDPPC perceives that educators must be equipped with up-to-date, relevant and sufficient information on data protection and privacy rights to be able to implement effective "e-learning platforms."

On the fourth point, the ICDPPC anticipates that a collaborative approach between privacy regulators and educational authorities will increase leverage,

[295] Global Privacy Assembly, *Resolution on E-Learning Platforms*

knowledge exchange, and resource maximisation. For British Columbia, it is important to consider the roles of school boards and the Ministry.

On the fifth point, the ICDPPC seeks to distinguish between appropriate and excessive reliance on consent. For the ICDPPC, the legal basis for the processing of student data should be determined by law or rules established by competent regulatory authorities wherever possible. Only if no such legal basis is available should parental consent, student consent, or both be obtained. The presumption is that withholding consent will not lead to a disadvantage of any student compared to his or her consenting peers.

On the sixth point, this policy should clarify appropriate uses of the e-learning platform and any consequences of using a personal device, especially when installing software or mobile applications.

The ICDPCC DEWG is an institutional forum, as noted above, through which the Privacy Commissioner may exchange best practices regarding online platforms and software application in schools. ICDPCC Resolutions' for data protection include the following statement: "Cooperate with each other and with the Digital Education Working Group to share resources, knowledge and best practices."[296]

In addition, the ICDPCC Resolution identifies specific issues that will most likely need to be considered and, in due course, acted upon by the Privacy Commissioner. These issues are partly the downstream consequences of the mandate of the Privacy Commissioner to enforce Students' Privacy Rights vis a vis public bodies in British Columbia. For example, the ICDPCC Resolution calls upon data protection authorities to "[u]se this Resolution to develop guidelines that assist educational authorities and e-learning platform providers and manufacturers in meeting their data protection and privacy obligations."[297] Translated into the technical and legal language of FOIPPA, the ICDPCC Resolution calls upon the Privacy Commissioner to issue Guidance that: assists public bodies, such as school boards, in making reasonable security arrangements

[296] Global Privacy Assembly, *Resolution on E-Learning Platforms*, at 7.
[297] Global Privacy Assembly, *Resolution on E-Learning Platforms.*

and ensures that any service providers, such as Google, comply with FOIPPA generally and respect students' privacy rights specifically.

Finally, the ICDPCC Resolution calls upon domestic data protection authorities to:

- Inform and raise awareness of the privacy risks and responsibilities of using internet platforms;
- Promote the ICDPCC Resolution and its recommendations with stakeholders and policy-makers in their jurisdictions; and
- Liaise with relevant civil society groups to promote and follow up on the Resolution.[298]

The inter-play of roles between the province, school boards, and the Privacy Commissioner is considered further in the conclusion to this report.

[298] Global Privacy Assembly, *Resolution on E-Learning Platforms.*

6. CONCLUSION

> *"On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other."* Stewart Brand (Author of *The Whole Earth Catalogue* and gadfly of Silicon Valley)

The above quote is from a conversation between Silicon Valley gadfly Stewart Brand and Microsoft co-founder Steve Wosniak at the world's first conference for hackers.[299] That conference – and the quote from Brand that has since been passed around popular culture and the internet in many different forms[300] – was an essential precursor to the information age in which we now live.[301]

In today's information age, our lives are documented in digital databases. These databases are composed of bits of our personal information, which when assembled together reveal a great deal about our personalities and preferences. These databases also determine, to an even greater extent, our place in society and the economy through automated decisions. For example, digital databases maintained by credit agencies may impact whether we get a car loan, a mortgage, a license, or even a job. Following the September 11, 2001 attacks, similar databases were used to determine whether certain groups of people were permitted to enter the United States. In light of the on-going Covid-19 pandemic, there is now intense debate about whether and how these databases will be used to track and trace contact between potentially infected people.[302]

---

[299] Steven Levy, *Hackers: Heroes of the computer revolution*. Anchor Press/Doubleday NY 1984.

[300] *"Hackers" and "Information Wants to Be Free" The most famous phrase in the book wasn't mine. And it wasn't in the book.Steven Levy, Nov 21, 2014 https://medium.com/backchannel/the-definitive-story-of-information-wants-to-be-free-a8d95427641c#.y7d0amvr3*

[301] The notion of an 'information age' is used metaphorically. For a relevant discussion. see the concepts of an infosphere and hyper history employed by Luciano Floridi, *The fourth revolution: How the infosphere is reshaping human reality*. OUP Oxford 2014

[302] Florian Schneider eds. *How Asia Confronts COVID-19 through Technology* online: Leiden University Asia Centre <https://leidenasiacentre.nl/en/how-asia-confronts-covid-19-through-technology-2/>.

In a society where digitalized information flows so freely and proliferates so rapidly, is it possible to protect privacy? This question is increasingly hard, if not impossible, to avoid. Indeed, Oxford University professor of philosophy Luciano Floridi describes online privacy as one of the most important issues of today's coming information age.[303]

As examined in this report, a material aspect of an information age is that once purely public services, such as K-12 education, are now increasingly being provided through cloud computing systems. Cloud computing is frequently marketed by private providers to public bodies. Section two of this report examined how one specific internet platform, i.e. Google's G Suite for Education, and the software applications that it makes available, are being used in every region of the province. Indeed, internet platforms offer education authorities an apparently free mechanism for outsourcing information technology services generally and software applications specifically.

There is no reason to doubt that cloud-based internet platforms and software applications targeted at the education sector can facilitate the use of new technologies, such as digital devices and the internet itself. They also facilitate a broader shift from paper-based to screen-based instruction as both student outputs and teacher evaluation can be digitized. But what is the cost to student privacy, and how can our public bodies ensure that this cost is not contrary to Canadian privacy law?

At the core of Canadian privacy law is information privacy, and the intimate connection between personal information and personal liberty. This connection is even more sacrosanct where the personal information belongs to children and is, thus, by its very nature, sensitive. In British Columbia, public sector use, disclosure, and collection of personal information is governed by FOIPPA.[304] Public education, meanwhile, is characterized by the historical bargain of provincial jurisdiction and local representation. The Ministry of Education administers policy and allocates budgetary resources while local school boards make and oversee the implementation of operational decisions. What this means in practice is that

[303] Luciano Floridi, *The fourth revolution: How the infosphere is reshaping human reality*
[304] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, *c. 165.*

school boards face increasing demands on finite resources, which may create a challenging environment for investing in information technology capacity and resources.

FOIPPA establishes quasi-constitutional information privacy rights for students in the public education system. This report has identified and examined three particularly salient forms of students' privacy rights:

- Right against Unauthorized Collection;
- Right against Unauthorized Use;
- Right against Unauthorized Disclosure.

A corollary to students' privacy rights is that public bodies' decisions and policies may create privacy risks. The province's public sector has specifically described a FOIPPA privacy risk as "something that could cause unauthorized collection, use or disclosure of personal information or result in any other contraventions of FOIPPA".[305]

The research conducted for this report has found a series of reasonably foreseeable privacy risks associated with existing patterns of software application usage in the province's public schools. These major privacy risks were examined in relation to available facts about usage of Google's G Suite for Education, and encompass: over collection of personal information and collection of sensitive personal information; unauthorized use in the form of unlawful processing, lack of transparency, lack of accountability, function creep, and a chilling effect; and, unauthorized disclosure, which is interlinked with concerns about storage of students' personal information in foreign jurisdictions including the United States.

Having recognized students' privacy rights and the scope of the major privacy risks, concerns persist about whether enough is being done to manage these risks.

---

[305] Ministry of Technology, Innovation and Citizens' Services, *Privacy Impact Assessment Guidelines* (2014), online: <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf >. See also, the current Ministry of Citizens' Services website, online <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments>.

The general principle in FOIPPA is that public bodies must make reasonable arrangements to protect the security of personal information. This obligation applies to public bodies even when personal information is in the custody of a service provider. The report therefore reviewed two risk management tools that should be used by a public body engaged in contracting out: a privacy impact assessment and a service agreement with privacy provisions.

It has been more than a decade since the Privacy Commissioner's landmark report on managing risks associated with outsourcing. It led to twenty specific recommendations that have been accepted in full by the provincial government. Concerns, however, persist about whether public bodies are fully prepared to manage the privacy risks that arise when services are contracted out to software applications and internet platforms through the SaaS cloud computing business model.

In early 2020, the COVID-19 emergency led to the temporary closure of schools and, in turn, the relaxation of certain privacy safeguards related to net-based platforms and applications.[306] In this respect, COVID-19 has, perhaps, had the unintended consequence of drawing attention to the use of platforms and applications in the public education system. Software applications and internet platforms are almost certainly going to be part of British Columbia's public education for the foreseeable future. As we collectively turn to shaping a post-state of emergency 'new normal', it is important that we no longer ignore the privacy concerns and risks associated with these technologies. Now is the time for all concerned stakeholders to think seriously about systematic solutions for managing risks and safeguarding students' privacy rights.

How can potentially incomplete compliance be most productively addressed?

In light of the inherently interconnected nature of online activity, one path to more effectively safeguarding students' privacy rights is to draw on emerging best practices from other jurisdictions and emerging transnational norms. Section 5 therefore introduced the IPC guide recommendations, IWGDPT

[306] *Ministerial Order No. M085* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085>; *Ministerial Order No. M180* online: <https://www.bclaws.ca/civix/document/id/mo/mo/2020_m180>

recommendations, the GPEN recommendations as well as the ICDPPC's *Resolution on E-Learning Platforms*. By way of conclusion, it is helpful to explore the application of these principles in the context of British Columbia's specific institutions and laws.

First and foremost, the ICDPPC is a global, membership driven organization that counts amongst its members not only Canada's federal Office of the Privacy Commissioner but also British Columbia's Privacy Commissioner. The Privacy Commissioner is a signatory to the ICDPPC's *Resolution on E-Learning Platforms* (although it has not, to date, been especially involved in the ICDPPC's Digital Education Working Group). To this extent, the Privacy Commissioner has already committed to using the *Resolution* as a starting point in formulating guidance to public bodies in the education sector so that they may fully comply with their privacy obligations. Through the *Resolution*, the Privacy Commissioner has also committed to raise awareness about the privacy risks to end-users and responsibilities of intermediary users in the cloud computing context; promote the *Resolution* and its recommendations with stakeholders and policy-makers in British Columbia; and, liaise with relevant civil society groups to promote and follow up on the *Resolution*. Therefore, it is reasonable to expect that the Privacy Commissioner should be proactively examining whether and to what extent the use of internet platforms and software applications in public schools may be consistent with FOIPPA compliance. The time for the Privacy Commissioner to take these actions is now.

Under the ICDPPC *Resolution* an additional six recommendations are addressed directly to educational authorities. In the context of the province's public education system, the implications are as follows: first, a collaborative approach should be taken between privacy regulators and educational authorities at both the local and provincial level. Second, teachers and other educators should have access to timely, relevant, and sufficient information on data protection and privacy rights; however, there also needs to be a clear allocation of roles and responsibilities so as to avoid the invidious situation where employees directly contract with a platform or application service provider. School board representatives with legal authority to contract with technology providers must be accountable for ensuring adequate privacy protections and should, accordingly, have substantive knowledge of British Columbia privacy laws. Finally, there is

strong support for distinguishing between appropriate and excessive reliance on consent. The presumption must be that withholding consent will not lead to a disadvantage for the student.

The IPC guide recommendations also identify a number of initiatives that are relevant. It contemplates, at the policy level, the development of criteria for evaluating, approving and supporting the use of online educational services. At the human resources level, the provision of privacy and security training and ongoing support for teachers and staff. In terms of students' privacy rights, IPC guide recommendations include the notification to students and parents about the personal information that may be handled by the online services and the reasons for handling it; and, allow for students or parents to opt out of online educational services, and provide other ways to deliver the same educational services. This final point is especially important and it points to what might, in due course, become a basic premise of evaluating the decision to contract out educational services: educational services can only be contracted out when the public body has a non-privacy invasive alternative that it makes available to students and parents.

The IWGDPT recommendations include: engaging service providers that offer sufficient guarantees to ensure that the privacy and data protection rights of students are adequately protected; and, implementing necessary technical and organizational measures before and while using the outsourced services. The GPEN recommendations also provide useful principles that merit consideration. For example, to provide timely ongoing guidance to students on appropriate uses of any online educational services. This may be contrasted to the current policy-based approach in some parts of the province where some school parts have stipulated acceptable and unacceptable uses of software applications without necessarily providing training or supervision. The GPEN recommendations also highlights the need to seek the involvement and express consent of parents and guardians.

It is on the basis of the above that the current report arrives at the specific recommendations indicated below.

RECOMMENDATIONS:

1. The Ministry of Education should play a more active role in supporting the procurement of cloud computing services. The Ministry's strategic role in the public education system and relatively sophisticated information technology capacity should be leveraged to maximize resources, exchange knowledge, and develop best practices for privacy risk management.
2. Privacy Commissioner should make use of the International Conference of Data Protection and Privacy Commissioners' ("ICDPPC") activities regarding online platforms in public schools. Specifically,
    a. Actively participate in the ICDPPC Digital Education Working Group's activities, including the questionnaire that was circulated by the French data protection authority and Canada's OPC in June 2019, so as to exchange best practices with other jurisdictions;
    b. In light of commitments and norms embodied in ICDPPC *Resolution*, formulate a guidance document for public bodies in the education sector so that they may fully comply with their privacy obligations when engaged in contracting out cloud computing services.
3. School boards should ensure they have information technology and privacy expertise necessary to:
    a. Conduct substantive privacy impact assessments on private sector providers of information technology services;
    b. Develop policies and procedures to assess, approve, and support the use of internet platforms and software applications without compromising students' privacy rights or shifting the privacy risk management burden;
    c. Provide training and support for teachers in respect of classroom technology and privacy;
    d. As required and appropriate, seek valid, informed and meaningful consent from individuals, i.e. students and guardians.
4. Ministry of Education and school boards should strengthen co-ordination to:
    a. Negotiate, as necessary, service agreements with service providers who may be unwilling to negotiate with individual school districts;

b. Establish a shared mechanism for rating and otherwise exchanging knowledge about internet platforms and software applications;
c. Maintain said mechanism while taking on-board feedback from students, guardians, and teachers.

FIPA BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

#103-1093 West Broadway
Vancouver B.C. V6H 1E2

p: 604.739.9788
e: fipa@fipa.bc.ca
w: fipa.bc.ca
tw: @bcfipa

ISBN 978-1-7772225-1-2