SPECIAL REPORT 23-03

The digital dilemma: Reflections on the OIPC Youth Forum

APRIL 2023
CANLII CITE: 2023 BCIPC 35
QUICKLAW CITE: [2023] B.C.I.P.C.D. NO. 35

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

On March 9, 2023, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) hosted the OIPC Youth Forum. A group of high school students from across British Columbia joined experts from the OIPC, the BC Civil Liberties Association, MediaSmarts, and special guest speaker, Cambridge Analytica whistleblower and social researcher Christopher Wylie, for a wide-ranging discussion on the privacy issues that impact students most.

Commissioner’s message

Today’s young people are the first to grow up in an all-encompassing digital environment – tethered to devices fuelled by ever sophisticated artificial intelligence that is linked globally.

Its impact on child and youth[1] development is not completely understood but the questions raised by this technological tsunami about potential harms and benefits, compel us as legislators, policy makers, regulators, and as a society to seek answers.

It is 40 years since the advent of the internet and nearly 20 years since the first major social media platform Facebook entered our lives. Tremendous advances in AI are now happening in a matter of months, not years and our laws continue to respond to these developments. However, we do not have the luxury of taking a decade-long wait-and-see approach: we cannot, as Christopher Wylie phrases it in this report, let our children be “guinea pigs” for the harms to come as untested, society-shifting technology is unleashed.

As a regulator, we’re bringing youth into the conversation. This report provides an overview of discussions we had one morning early in March 2023 with a group of engaged, thoughtful high school students from across the province. The online meeting explored some big ideas and I hope that this report reflects the substance of some of them and the high level of engagement that these young people brought to the table. I was impressed by their considerate comments, their ability to relate what was discussed to their own experiences, and, importantly, their desire to ask questions and learn more about their privacy rights.

I would like to thank my staff who were involved in preparing the Youth Forum and this report, as well as Christopher Wylie, Mara Selanders from the BCCLA, Matthew Johnson from MediaSmarts and, of course, the students who took the time out of their busy school day to join us for such a rich and thoughtful discussion.

[1] In this paper, we refer to both “children” and “youth”. By “children” we generally mean those 12 and younger. By youth, we generally mean those over age 12. We make the distinction between “children” and “youth” to delineate among different groups of young people, however all the work that we are planning for a “Children’s Code” would apply to children as well as to youth.

Youth are ‘guinea pigs’ for untested, dangerous tech

Christopher Wylie, social researcher, whistleblower, author

Young people today are going to be the first generation in history to have every aspect of their lives recorded in some way, a ceaseless stream of personal information from cradle to grave, says Christopher Wylie. Yet there are more laws and regulations in place for a company to comply with before it sells a toaster than before it can unleash a social media platform, or a game to millions of children.

Christopher, who was born and raised in Victoria BC, came to global prominence as the whistleblower behind the 2018 Cambridge Analytica scandal. He worked with the UK’s Office of the Information Commissioner, including with Commissioner McEvoy, who was then seconded to that office, and *The Guardian* and *The New York Times* newspapers to expose how the company harvested the personal data of millions of Facebook users without their consent, psychologically profiling them to influence the 2016 US presidential election campaign, and the UK Brexit campaign.

*Christopher Wylie, author of Mindf*ck: Cambridge Analytica and the Plot to Break America*

Those experiences informed Christopher’s perspective on a tech world where the ethos is all too often to “move fast and break things.”[2] But what about when those “things” are people’s lives, Christopher asked, specifically those of young people coming of age amid the proliferation of this technology?

‘False narrative of choice’

Young people are immersed in social platforms, Christopher said, because that’s what is expected of them – whether it’s a social platform to talk to friends, LinkedIn to apply for a job, or Google for search functions and many other services.

> “There’s a false narrative that you have a choice – that you don’t have to use these platforms. If you don’t, how do you engage with modern society?” – Christopher Wylie

[2] Attribution to this motto is usually given to Mark Zuckerberg of Meta and has been widely adopted by many in the tech industry as a way to express prioritizing innovation over everything else. For more, see: https://en.wikipedia.org/wiki/Move_fast_and_break_things.

One of the Youth Forum student participants said that young people are so "acclimatized" to these platforms in their school and personal lives, that there is often little thought given to the personal information shared in individual instances.

"When you download an app, there is really fine print. You don't really have a choice," they[3] said. "When you get to school you're on a computer, you accept cookies, say yes even if you don't understand."

The student added that young people also often aren't aware of what happens to their personal information when they provide it online, something that they would like to see change. "It's important for our generation to know. If a stranger came up and asked to take 50 photos of you and save it to give to other people, you'd say obviously not."

Christopher, likewise, underscored the importance of young people understanding and recognizing the importance of their privacy rights online.

"Privacy is about personal growth and being in charge of your life," he said. "As soon as we remove the ability to decide what information is disclosed, you are no longer in charge of what you reveal about yourself in those situations."

People are slowly letting go of that power as they engage more with these platforms, he said. "Companies and platforms will make choices about who you are. Everything is preselected by an algorithm that has decided how to classify you."

Another student commented on addictive algorithms designed to keep people on their devices.

> "We're kind of immune to it. It's second nature. On IG [Instagram] and iPhone, text bubbles pop up and you wait to hear from [the other person] and that becomes addictive, too. We can see that the tech is designed to be addictive and they take advantage of our lack of knowledge about that." – Student participant

The student agreed that it was important to have more discussions about the personal information young people are sharing online.

Christopher said the onus should not be on young people to foresee every possible misuse of the information they provide on these platforms.

[3] We did not ask youth forum participants for their pronouns therefore for this report we are referring to any of the participants as "they/them".

"You don't know and you shouldn't have to know. You should be able to use a service and not have some consequence where now your photos are owned by some random company that might use them 20 years from now," he said. "Until government steps in, you might get a situation where the things you put on a platform get used in some unforeseen way that affects you in a way you could not have known."

Without safeguards, harms proliferate on these platforms.

AI, regulation, and pushing for change

Christopher said a harm mitigation approach – the type of approach standard in most consumer-facing industries – is especially important amid the rapid emergence of AI.

"We're just at the precipice of scaled use of AI becoming a part of our everyday lives. Where is this going in the next 10-20 years?" he asked. "What happens if you start watching TV and the TV is watching you and talking to appliances in the kitchen … all devices watching you and shaping the information around you to make you a better consumer, voter, to shape you [into who] someone wants you to be?"

There is no doubt that AI is going to be a major part of young people's lives: the jobs they get, the people they meet, the schools they get into, whether they get a mortgage. "All of these important things are going to be mediated by AI and currently there are no obligations by makers to consider your wellbeing and whether it harms you," he told students.

What happens, he asked, when there is racial bias embedded into the AI, for example, or when there is no transparency around how the AI arrived at a decision.

> "You're the first generation that is going through it – you're the guinea pigs. If that makes you uncomfortable, write a letter and go talk to your MP [asking], 'Why is it that these technologies are going to impact my life and there are no rules." – Christopher Wylie

He said it's important for youth to ask questions about the tech companies that play such an important role in shaping their lives, and society. "What are the underlying motivations of these platforms and what are they doing to me? What kind of society do you want to live in and what do you want the tech companies to do to reflect that or not do?"

Privacy at school

Mara Selanders, Lawyer, BC Civil Liberties Association (BCCLA)

What expectations can students have when it comes to their privacy rights at school? Can administrators search their smartphones, for example? The answers to these questions generated surprise and a lively discussion at the OIPC Youth Forum.

Mara Selanders, a community lawyer with the BCCLA, provided an overview of the complex world of students' privacy at school – and the thorny issue of how laws and legal precedent that developed decades ago are applied in today's digital context.

Mara spoke about a BCCLA project that started with law student volunteers researching digital privacy rights in schools and finding "a massive gap in the law surrounding the rights of students regarding search and seizure in schools."

"While students do have a right to privacy while in school, that right is limited because the Supreme Court of Canada decided back in 1998 that the responsibility of school administrators to ensure the safety and well-being of the student body as a whole is greater than an individual student's right in certain circumstances," Mara said.[4]

Supreme Court of Canada decisions are binding across the country. The only ruling regarding searches of students since that time was in 2008, "far preceding the rise of smartphone use," Mara said.[5]

"To date, there have been no further [Supreme Court of Canada] decisions on the matter," she said, "meaning that the guidance given from our courts to our lawmakers on the topic of searching students has yet to consider our present-day context of student smartphone use and therefore fails to account for some significant differences."

Mara said the main difference here is the amount of personal information kept on smartphones.

[4] Supreme Court of Canada: R. v. M (M.R.) https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1666/index.do

[5] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1666/index.do

"Just think about how big your backpack or locker would have to be to contain all of the personal information stored on your phone or think about how many students back in 1998 would be bringing their personal, handwritten diary with them to school," she said. "Now think about how much easier and more efficient it is to search through that same personal content on your phone!"

Mara said that while the BCCLA wants schools to be safe, this "massive change in context" calls for updated direction from the courts and that "the traditional approach to search and seizure for students is in desperate need of an update.

Clip from BCCLA's video: Personal Electronic Device Searches in classrooms - https://www.youtube.com/watch?v=ONpuELdbRHM

One student commented that they had been to different high schools in the province and remained unaware that their phone could be searched. If they had known that, they would never bring their smartphone to school. "The same as you wouldn't bring a private diary to school and give that to someone willingly," they said.

Moreover, just putting these rules in schools' codes of conduct is "not enough," the student said, likening it to the terms and conditions in an app that nobody reads. "There should be an obligation to tell students. It's not fair that schools can hide this information and the power they have over students."

Mara agreed. "The onus is on students to track down rights rather than on school administrators to be transparent." She says that at a minimum, students should know that they cannot legally be randomly searched or in every circumstance.

The BCCLA calls for searches to be carried out in a sensitive manner that is minimally intrusive to the student and based on evidence of a possible violation – for example a report from a student that a classmate was carrying a weapon. The extent of the search should be justified by the possible rule infraction, threat, or concern. "This essentially means that the greater the overall safety risk to the student body, the more ground the search can cover (possibly including a cell phone)."

Mara said that challenging existing laws and precedents about student searches by school administrators is difficult, requiring a significant financial and time commitment. "Further, judges have been slow to engage with technology change generally and, in many cases, have been hesitant to acknowledge the impacts that technological change has had on privacy rights."

In the meantime, Mara encouraged students to reach out to their schools or school districts and ask if a technology use policy or code of conduct addresses search and seizure in the context of electronic devices.

Ethics and privacy online

Matthew Johnson, Director of Education, MediaSmarts

Today's youth constantly face decisions about how to handle personal information online – both their own and that of others.

Matthew Johnson, Director of Education with MediaSmarts, a Canadian charitable organization dedicated to media literacy,[6] encouraged the participants to think about the wider ramifications of their online activity that are often obscure in the moment. These considerations range from ethical choices – is this information mine to share? Am I hurting anyone by doing so? – to understanding how our interactions with major platforms are driven by commercial interests predicated on endless engagement to reap advertising profit.

"There can be a lot of eyes on what you post online. That includes people you know about – your friends, your family, and other people you expect to see what you've posted – but also people you don't know about," Matthew said. "Every single one of Canadian kids' top apps and websites is a for-profit business, and almost all of those make at least some of their money by collecting information about you."

That information can come from the personal information people provide when they register for a service or their actions while using that service. "They feed that information into algorithms that put it together to make guesses about things they might not know, like your race, your gender, whether you have a disability, and so on."

People might be aware that this kind of information is used to keep people engaged for longer periods or to target ads to them. While these uses may seem innocuous, Matthew said there

[6] https://mediasmarts.ca/about-us

are more serious implications involved. "Think for a second: what if you didn't see an ad for a job you would have been perfect for, or didn't find out about a show you'd really like, because the algorithm [decided] you wouldn't be interested?"

In response to a question from a student about what platform tends to "use or abuse" your information the most, Matthew said "they're roughly all the same" and emphasized that there is no connection between how a social network may let you control privacy with other users and how that network respects your personal information when it uses information for its own purposes, such as to improve a service.

Likewise, another student commented on the challenges of navigating privacy permissions for different apps. "When we use apps, we're forced to agree to these terms, use cookies, use our location," they said. The student asked what young people should keep in mind when it comes to these permissions.

Matthew said that there are times when it makes sense to give apps access – like when you're using a GPS, but he advises taking steps to limit data collection. "Because these companies own multiple platforms, there's no guarantee that the information collected about you [in one context] could be used in other ways [that you never intended]," he said. "Don't turn everything off but think carefully and be stingy with your personal information."

Making ethical choices

Even the most stringent privacy settings can offer only a certain level of protection online. "Privacy settings only work so long as the people who do see what you post make good choices about it," Matthew said. "That's why it's important for all of us to respect other people's privacy."

He said that means taking a moment before posting on social media and asking questions: "Did they mean for it to be shared? Did they have permission from anyone else who's in it? How would I feel if somebody shared something like this with me in it?"

Tips to protect privacy online

Limit your audience: Most social network apps have privacy settings that allow you to limit who sees your posts. On many apps, you can limit audiences both for individual posts as well as for anything you post.

Default level of privacy: Set this so that only the people you know and trust can see the things you post.

Limit collection of personal information: Some apps will let you choose what information is collected about you and how it's used.

Privacy check-ins: Check back on your settings every now and then – sometimes these things get 'accidentally' turned back on.

Privacy settings on devices: You can control which apps can access your camera, microphone and GPS. This is easier to navigate on iPhones or iPads, where you'll need to give apps permission to track you, for example. However, Android users can download the DuckDuckGo app and turn on app tracking protection. Browser extensions like Privacy Badger can do the same for browsers like Chrome or Firefox.

“Even better, ask everyone who’s in a photo or video if they’re okay with you sharing it. Be clear who will see it and what you’ll do to limit the audience,” he said. “Don’t guess whether or not they’d say yes. There might be reasons why somebody might not want something shared that you’re not aware of.”

“Remember, once something is online it’s out of your control – so make good choices about your privacy and others.”

Next steps: Towards a Children’s Code in BC

The OIPC is in the early stages of developing a Children’s Code to clarify organizations’ obligations when it comes to handling children’s personal information to ensure they are complying with the *Personal Information Protection Act* (PIPA)’s reasonableness requirements, and other statutory obligations.

Here are some key points being considered as the code develops.

Companies should be required to:

1. Put the best interests of the child first; and
2. Complete a privacy impact assessment of their initiatives.

When developing online services that are likely to be accessed by a child in BC, or who is from BC, companies should be prohibited from:

- Using nudge techniques (for example, making a button that says yes in big bright letters and a smaller black and white button that says no.)
- Sharing children’s data with third parties, except contractors, even with consent, unless there is a compelling reason to do so that is in the best interests of the child (like sharing it with the police for an investigation); and
- Collecting a child’s precise location.

There are many governments and privacy regulators around the world that are examining how to strengthen laws to help protect young people online from being harmed by dangerous tricks and designs that some technology companies use to increase their profits at the cost of young people’s mental, physical, and financial well-being.

Conclusion

My office promotes and protects British Columbians' privacy rights by enforcing the public sector *Freedom of Information and Protection of Privacy Act* (FIPPA) and the private sector *Personal Information Protection Act* (PIPA). These laws were enacted long before social media became ubiquitous and when so much of our lives were spent online, but they are based on fundamental principles that span time and technology.

Today's youth are facing more varied and complex challenges to these rights than any generation before them. That is because so much of our lives are recorded on phones, computers, surveillance cameras, and other devices to a much greater extent than any humans before them. Bringing youth into the conversation is essential if we are to better understand and respond to the threats that such reams of data pose to our individual mental health and the collective health of our societies.

While our legislation is based on fundamentally important privacy values like accountability, there is also a need for governments to enact specific safeguards to meet the challenges posed by increasingly sophisticated technologies. To this end, my office is working on developing a Children's Code. As this report details, similar Codes are already in effect in other jurisdictions. What these codes provide is "rules of the road" for businesses that process children's personal information – clear guidelines that are more specific and focused on addressing the unique harms that children face when they engage with online platforms. I am excited about this work and look forward to sharing more as it develops.

The Code and our commitment to continuing our conversation with BC youth are steps toward the wider goal of ensuring that today's youth are able to enjoy the tremendous and exciting potential of technology while minimizing opportunities for bad actors to manipulate youth for their own gains.

I hope this report provides an opportunity for reflection on these important issues.

Resources

Chris Wylie: Mindf*ck: Cambridge Analytica and The Plot to Break America:

https://www.penguinrandomhouse.com/books/604375/mindfck-by-christopher-wylie/

BCCLA

- Video*: Personal Electronic Device Searches in Classrooms* - https://www.youtube.com/watch?v=ONpuELdbRHM
- Additional resources: https://bccla.org/our_work/edevices/

Media Smarts: https://mediasmarts.ca/

Children's Code

Other jurisdictions that currently have some form of Children's Code include:

United Nations Convention on the Rights of the Child: Adopted in 1989, the UNCRC is an international treaty outlining children's rights, including privacy rights. Article 16 of the UNCRC, says: "Children have the right to protection from interference with privacy, family, home and correspondence, and from attacks on their character or reputation."[7]

GDPR: Article 8 and Recitals (38) and (58) of the European Union's General Data Protection Regulation include special rules for governments and companies that use children's personal information. In addition, companies in the EU must take reasonable steps to ensure that a child is not pretending to be older than they are in order to get around the requirements for parental consent.[8]

UK: The Age Appropriate Design Code, or Children's Code, published by the Information Commissioner's Office in 2021 sets standards for how companies can process children's data.[9]

Ireland: In 2021, the Data Protection Commission of Ireland published its "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing." These "Fundamentals" provide companies processing children's data in Ireland with rules on processing children's information in Ireland.[10]

California: One major initiative is a new law that will require companies to design apps and websites without using techniques to trick individuals into clicking something or taking some action because the design has strongly led them to do it.[11]

[7] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[8] https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en.

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/

[10] https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[11] For more information, please see: https://www.gov.ca.gov/2022/09/15/governor-newsom-signs-first-in-nation-bill-protecting-childrens-online-data-and-privacy/ .