Privacy in online learning/teaching

Preliminary issues paper

Privacy Foundation New Zealand, Wellington, August 2022

Dr Marcin Betkier, with the contribution from members of the Foundation Committee and Children's Privacy Working Group

The Privacy Foundation New Zealand, as part of its programme for 2022, has commenced an investigation into the privacy of tamariki/children and young people at New Zealand schools with a focus on the shift towards an online learning/teaching environment.

The aim of the investigation

The Privacy Foundation would like to ensure that our children are brought up in a safe educational environment in which their privacy is respected and their personal information is used only for the goals of their education and in their best interest.

In this regard, we are seeking more information from all stakeholders, including the public, about the organisation of the online learning environment, the software used by Aotearoa New Zealand schools (for example, Google Workspace for Education, Microsoft Office 365), methods and tools used to protect children and young people's privacy and their personal information, and concerns regarding children's privacy when they engage with activities related to online learning at schools and at home.

The aim of this paper

This paper is a list of preliminary issues that have been discovered during the Foundation's investigation until August 2022. During that time, we have undertaken preliminary conversations with the stakeholders in the education sector: schools, the Ministry of Education, Netsafe, the New Zealand School Trustees Association and the Office of the Privacy Commissioner. We also have sent Official Information Act requests to the Ministry of Education and to the Office of the Privacy Commissioner. (All the requests can be found on the Foundation's website.

The goal of the paper is to list the potential issues, present them to a wider audience and stimulate further discussion around them. In the course of further investigation, some of those issues may be found to not exist. Also, there may be other issues which will arise. So, the below is our best assessment as at August 2022.

If you would like to send us any comments about the investigation or this document, go to https://www.privacyfoundation.nz/campaigns/

Introduction

Online learning has seen an exponential rise in recent years, particularly with the global pandemic. In a disrupted environment, schools and kura face considerable challenges in providing safe, equitable learning. It is acknowledged that software and digital technologies are an enabler for improved education outcomes. The software and IT tools however present significant privacy risks. Below we present the potential issues we have identified. We encourage further exploration and dialogue, to identify practical mitigations, resources and supports.

Potential issues at the school / children level

1. **Tracking and profiling of children**

    a. Personal information is collected and used for education, but sometimes the collection is either not necessary for that purpose or not proportional (e.g. the use of biometrics or behavioural data may be not necessary)
    b. Personal information is collected for purposes outside education in schools (e.g. research, analytics, profiling children and whānau, tracking them outside the school context)
    c. Personal information is collected directly for commercial purposes (advertising, monetising otherwise, e.g. data sharing with third parties)

    The collection and processing of children's data should always be in their best interest. At schools, it should be limited to the necessary and clearly identified educational goals and the school's legislative obligations, which we acknowledge include student wellbeing and safety and Te Tiriti obligations. The categories above describe the use of data that is outside those goals.

    Preliminary analysis of the terms and conditions of some agreements with platform service providers show that they do not limit the collection to the best interests of the child and they allow the children's personal information to be used for commercial purposes and sharing with third parties. Some software providers declare not using the collected children data for 'advertising purposes' in some of their services, but that still leaves a huge space for other commercial uses and advertising in so-called 'additional services'. More research and in-depth discussion with those providers are necessary to explain that.

    The online tracking in educational software tools creates a pool of data about children (effectively, profiling them) that may be used outside of education and maybe even used commercially. That commercial use could be either by directly using data for

advertising to children, or by using data with third parties or to profile other people – other children, their whānau, etc.

Software used to track children's progress in school can also record deeply personal information (or attach labels through profiling) which have implications during and beyond school, e.g. disruptive, intellectual challenge or emotional disturbance.

2. **Combining data across services and products, often linked with upselling / cross-selling**

    a. 'Data leak' - linking information collected for online learning with the collection of information from additional commercial services/products.
    b. Linking children's data to data about other people outside the educational context – whānau, friends, etc.
    c. Lack of choice of 'additional' commercial products or services (e.g. the use of particular providers is required)

Those additional services or products may include:

- equipment (e.g. Chrome books),
- web browsers (e.g. Chrome, Edge, Safari),
- email services (e.g. Gmail),
- video sharing or streaming services (e.g. YouTube),
- maps (Google Maps, Apple Maps),
- search services (e.g. Google Search, Microsoft Bing),
- location-based services (other than maps),
- business services for schools,
- other Internet services.

Combining the information collected among services and across a child's devices seems to be a common practice. In that way, the personal data collected in the educational context may be linked to other data (e.g. other 'accounts' of the child) and to other people, which effectively enables the use of educational data in other contexts, outside the 'best interest of a child' category. Further, a child's data may be combined with data from other users of the "child's device" (where devices are shared), and lead to errors in data and insights derived from that data that affect the child.

Also, the other way around, children's personal information collected for non-educational purposes may then be used to inform the learning process for children, e.g. behavioural data, websites visited, etc.

A separate issue could be the actual choice of products and services which may be limited, for example, if the school chooses a particular provider of equipment, devices and/or services. That may also cause equity or accessibility problems.

3. **Influencing children and families or otherwise creating harm**

   Children may be subject to marketing actions targeted at them. Those actions, that are not limited to serving profiled advertisement, may rely on influencing their behaviour. That can be reinforced by the use of addiction mechanisms (e.g. the use of social media is addictive), gamification (using game-based logic to engage children) or, for example, the use of children influencers. Possible negative effects are: influencing children to buy /use unhealthy products (leading to conditions such as obesity), inducing habits that are preventing their normal development (e.g. overusing electronic devices that are supposed to be used for education), or exposing children to fringe/ extreme worldviews induced by the 'virality' of such views in online platforms.

   Children do not understand the commercial context of the information and are not capable of exercising judgment to distinguish fiction, reality, and advertisement strategies across the services. Monetisation mechanisms that may be questionable for adults are even less acceptable for children.

4. **Creating unsafe digital environment**

   It seems that the online learning environment:

   a. Is unequal in terms of power – children, parents, and schools can only adhere to the contracts imposed by online service providers. They have no real choice.
   b. Blurs the private sphere of children and their whānau, the educational sphere and the commercial sphere. That possibly is not a safe environment in which children can freely develop, make mistakes, and develop their self-confidence and identity. That can be a surveillance environment that records their activities and keeps their data for future and unknown use, which creates risks and limits children's choices.
   c. Exposes the children to risks, and undermines their development and evolving capabilities

   See point 3 above.

Additionally, the children may be 'normalised' to use devices and internet platforms that can be addictive and can negatively impact their health. That includes social media platforms that are often optimised on increasing the 'virality' of the content. Potential psychological harm includes anxiety, addiction, compulsion, device dependence, limiting the time for sleep and diminishing children's creativity, capacity to memorise, and autonomy. That lowers their self-confidence and the ability to be independent and autonomous individuals. As a result, their education chances may be diminished. An environment that is deprived of privacy may also foster cyberbulling and predatorial activities.

5. **Disclosure of personal data to third parties**

    a. In the advertisement 'food chain' (e.g. in the process of determining what advertisement is to be displayed in so-called Real-Time Bidding).
    b. Contractors and subcontractors.
    c. Secondary use of that data within and outside purposes of collection.

    If the personal data of children and young people is shared in any 'digital ecosystem'[1] that increases the number of entities that are 'custodians' of that sensitive content. That increases the risk of misuse of that data by any of them and the 'secondary' use of that data for purposes other than those communicated during the collection.

6. **Security risks of those data – exposure to harm if data leaks**

    The educational systems may be collecting a lot of data about children, as particularly vulnerable individuals. That might include their biometric and behavioural data. Security of that data is very important. Wide sharing of data in the 'digital ecosystem' may exacerbate the risks of leaking those data to some 'bad actors' who may use them against the children.

7. **Cross-border transfers of personal data to other jurisdictions (also without adequate privacy laws)**

    Sharing data outside the jurisdictional boundaries increases the risks if other jurisdictions offer a lower level of data protection. For example, the United States does not have any federal level privacy law that covers the private sector. Many of the states do not have any state-level privacy laws at all. It is often unclear and not transparent which laws apply to the contracts between the schools and Kura and overseas online platforms and how their potential commitments on those markets apply in New Zealand. As a result, it is harder and more costly for individuals to start any legal actions against companies and/or organisations that are overseas.

    Finally, there are legal requirements in the Privacy Act 2020 for transferring data abroad which should be fulfilled. Our preliminary analysis shows that many of the educational services providers offer their services from abroad, keep the data about children abroad and offer higher standards of privacy protection overseas.

[1] A group of interconnected information technology systems.

8. Lack of transparency

Looking at the complexity of the learning ecosystem and the level of complication of the Terms and Conditions of the services it is disputable whether children, their parents/guardians and schools have a full picture of:

a. what data is collected,
b. for what purposes,
c. by whom and where it is kept,
d. what the default collection settings are – opt-in or opt-out, any Privacy by design and/or Privacy by default approach,
e. how they can act to limit that collection.

If there is little transparency, people involved in the process may be unaware of the risks. Therefore, they can do little to mitigate those risks.
The requirements of the Privacy Act 2020 should be verified.

9. Lack of agency / opportunity to avoid collection

Even if the information about the collection is given, it may be hard to avoid an extensive privacy invasion. This is because the agreements for the provision of software may be adhesive – i.e., it is not possible to change these, and the agreements are non-negotiable from the perspective of schools, parents/guardians and children. It seems that the agreements entered into by the Ministry of Education are non-negotiable for schools.

Also, the software may not provide the option of limiting data collection to what is necessary for education and the primary reasons why information is collected by schools and kura. Further, the practice seems to be to direct children and parents to general service 'privacy controls' some of which have been found to be misleading overseas.[2]

10. Pedagogical issues

a. Teaching our children improper / insecure behaviour – exposure to risks.
b. Teaching them that their privacy is not important and has to be foregone for other goals.
c. Teaching them that they do not have anything to say about their data – the wrong digital citizenship model.

[2] For example, Australian Competition and Consumer Commission "Google misled consumers about the collection and use of location data" (16 April 2021) Australian Competition and Consumer Commission <www.accc.gov.au>.

d. Putting them in the position of clients of big international corporations with questionable business models and ‘normalises’ that at a very young age.

Those issues should not be underestimated. It is the goal of the educational system to bring up new citizens, aware and ready to be critical of the world. The educational environment in which children are forced to use privacy-invasive software achieves exactly the opposite. It ‘normalises’ surveillance and lack of privacy, complacency and the environment full of privacy and security risks.

General or systemic issues

1. Exercise of responsibility for privacy in online teaching/learning at New Zealand schools

The governance model of online learning seems to be deficient. The schools and kura that are responsible for choosing and using the online learning platforms have no power and expertise to make privacy-preserving choices. Also, the organisations that are supposed to help them have not been involved in order to analyse the issues and remedy any identified problems.

The schools and kura (and their boards of trustees) are ultimately responsible for choosing the educational tools to teach children. That includes software and hardware for online teaching and learning. Also, the New Zealand Schools Trustees Association provides advice, support and professional development to school boards, which includes board compliance with the requirements of the Privacy Act 2020.

However, those organisations have limited resources, technical expertise and agency to make privacy-preserving choices in the complex and dynamic world of global digital services. Further, the schools do not have the power to negotiate agreements with service providers. Some of those agreements (with Microsoft and Google) have been negotiated by the Ministry of Education and the schools simply adhere to them. The schools most probably have no tools to avoid the collection of personal information from children, sharing it within digital ecosystems and further reusing it for commercial purposes.

Further, from our preliminary findings, it looks like the Ministry of Education never analysed the privacy of online learning in terms of its compliance with the Privacy Act 2020 (or its predecessors) or assessed privacy risks. The agreements they entered into were never specifically audited or checked against privacy risks for children. It seems that they relied on the fact that they directly contracted with those vendors under the New Zealand law, on their overseas commitments and the Terms and Conditions of their services.

The Privacy Commissioner provides advice about privacy and also monitors and examines the impact that technology has on privacy. But, from our preliminary findings, it seems that the Office of the Privacy Commissioner had no particular focus or research on privacy in online learning. That may be understandable if we look at the number of privacy-related problems that had to be taken care of in the pandemic and the Office’s strategic work programme.

However, all of that infers that schools received no support from the sector in exercising their responsibility for children's privacy in the online learning environment. Also, that the governance model assigns responsibility to schools but gives them no means to bear that responsibility.

2. Lacking policy on privacy in online learning / teaching

It seems there is no policy that covers privacy in online teaching and learning. In times in which schools had to suddenly shift towards using online platforms to continue delivering education, there was no guidance related to avoiding privacy risks. The existing policy documents relating to privacy at schools cover only general privacy requirements with the Privacy Act 2020. The issue is not that there is no specific policy document about online learning. Looking at the information gathered until today, there seems to be no policy on that topic at all.

The educational software used in New Zealand should be verified against its compliance with New Zealand law and checked against the privacy and security risks. However, it appears probable, that no one verifies whether the online teaching software incorporates privacy-invasive functionality which may cause harm to children (see the 'potential issues' above). That remains true for the software provided under the agreements with the Ministry of Education. Also, no institution monitors the changes in that software and ensures that the level of service is maintained across the time.

3. Deficient mechanism of authorisation

It seems that ultimately the use of software, data collection and sharing in the digital ecosystem is justified by consent that is expressed by children or parents. However, in the online learning / teaching context:

- with particularly vulnerable individuals (children),
- with widespread data collection and use,
- with the opacity of the digital platforms, imbalance of expertise and knowledge about what personal information is collected and how it is used, and
- with the imbalance of power arising from both,
    - the digital environment and the existing privacy-invasive business models, and
    - the educational environment in which children are supposed to use the same tools for learning,

the use of consent as a moral, contractual, and sometimes legal authorisation for personal information processing (collection, use, transferring and/or sharing) should be questioned. It seems that children are often put in the position in which they must accept the terms and conditions of the use of software that is necessary for their education. But, all the factors listed above suggest they are neither capable of understanding the implications of that acceptance, nor really given the choice. This is not consent.

Data practices should not be justified by the questionable consent of individuals, or even institutions that cannot change the way the software works and can only adhere to the proposed terms and conditions. Privacy by design and by default seems to be a much better model for the educational sector. In our view, the government should implement a policy of imposing privacy-preserving settings on the educational software providers.

A reminder: We are seeking your feedback. If you would like to send us any comments about the investigation or this document, go to:
https://www.privacyfoundation.nz/campaigns/

Bibliography:

Human Rights Watch. "'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic," 2022.
Ministry of Education. "Education for the Digital Age, Case for Change and Next Steps" June 2018.
Ministry of Education. "Educational System Digital Strategy 2015-20. Transforming Education for the Digital Age" February 2016.
"Governments Harm Children's Rights in Online Learning." *Human Rights Watch*, May 25, 2022.
Hartung, Pedro. "The Children's Rights-by-Design Standard for Data Use by Tech Companies." *UNICEF Issue Brief* 5.
"FTC to Crack Down on Companies That Illegally Surveil Children Learning Online." *Federal Trade Commission*, May 19, 2022.
United Nations. Convention on the Rights of the Child. November 20, 1989.
New Mexico v Google LLC, Case 1:20-cv-00143, Statement of complaint 20/02/2020.
The Office of the Privacy Commissioner "Safeguarding Children's Data Privacy in a Digital World," May 9, 2022.
The Office of the Privacy Commissioner "Workshop: Privacy for Schools," May 11, 2022.
"DPIA on the Use of Google G Suite (Enterprise) for Education," 2021.
"Update DPIA Report Google Workspace for Education," 2021.
"New DPIA on Microsoft Office and Windows Software: Still Privacy Risks Remaining - Blogpost." accessed March 9, 2022.
"New DPIA for the Dutch Government and Universities on Microsoft Teams, OneDrive and SharePoint Online - Blogpost." accessed March 9, 2022

Aotearoa EdTech Excellence Report 2021 – available at: https://edtechnz.org.nz/wp-content/uploads/sites/7/2021/12/Aotearoa-EdTech-Report-2021_digital_new.pdf

Regan, P. M., & Steeves, V. (2019). Education, privacy, and big data algorithms: Taking the persons out of personalized learning. *First Monday*.

Akgun, S., & Greenhow, C. (2021). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, 1-10.

Apps et al., 2021, Edtech is treating students like products. Here's how we can protect children's digital rights, The Conversation (June 10, 2022)
https://policies.google.com/privacy?hl=en-US
https://www.microsoft.com/en-nz/servicesagreement/