12 March 2020
Killara NSW
newsmedia@vivaldi.net

Data Risk Assessment: An Open Letter to NSW Department of Education

To the Minister of Education, Sarah Mitchell and
The Secretary of NSW Department of Education, Mark Scott

As a parent and teacher I am concerned with recent developments I have seen with data handling and I am uncomfortable with increasing influence of data companies within NSW Department of Education. I will start with a recent Education trade show I went to recently in Sydney, it highlights some of the conflict of interests that take place in our corporatised education system especially at the top. I will than expand on the direct short term and long term risks to our children.

This is an open letter that will be available indefinitely on the *ReleaseTheFuture.com* for reference. It will also help parents be better informed on their expectations of privacy and the risks that their children could be exposed to. They may have given no informed consent for their children to be exposed to the risks below.

The Department with its highly centralised planning strategy could make it a soft target for big data companies who could use influencers, pseudo conferences and pseudo training and of course one on one lobbying.

Terrapinn appears to be an arm of and endorsed by NSW Department of Education

Last year I went to a NSW Terrapinn event which gave all the appearances that it was supported by the NSW Department of Education all the exhibitors, it seemed to be endorsed by the Department. This is how it would appear to the busy teacher. On registration sign-up; to further validate the Departments apparent enablement of these commercial vendors sales pitches, teachers are offered an educational certificate to enable them keep their Professional Develoment (PD) teaching valid – it now appears that our hallowed teacher development is just a marketing opportunity for vendors opening up commercial interests to enter our classrooms. The Department Secretary Mark Scott also chose to give his inaugural keynote talk at a Terrapinn event.

Teachers Used as Google Influencers

What I saw there was highly targeted training taking place. Department Teachers are used and engaged as influencers on the Google stand, exploited as apparent trusted voices but cynically harnessed by Google on their stand to promote their agenda to get into our classrooms. However Google could appear to have a **bigger picture strategy to groom our children** to freely give away their data and to portray themselves as as a safe place for our children psychometric data. This tactic, the use of community trusted influencers like teachers and Doctors, was the same tactic used by the father of PR Edward Bernays where famously in the 1950's he successfully got women to smoke by using, in part, trusted Doctors as influencers as agents of change.

Googles primary business model is data collection and exploitation. When I asked them on their stand about the issue of the long therm privacy the NSW DoE influencer teachers on the Google stand quoted a mother-hood statement on privacy as if they were Google employees and one of the teachers even thought that a concern for the long term safety of our childrens data was funny. I have noted that in public forums Google is hostile to legitimate concerns of long term abuses of data and they attempt to de-platform anyone who even asks a question on the issue.

Teachers Used as Microsoft Influencers

On the Microsoft stand there was a teacher from my sons school, Killara High, who when I asked during his presentation about the serious historical misuses of data, answered the question as if his answer was Microsoft policy. He was a Department employee, no caveats that he was not a representative of Microsoft.

In the previous year I saw Microsoft promoting facial recognition in the classroom.

School is about Socialisation

School is about socialisation, Google understands that. That is why they have put so much effort into education. Having Google in the classroom makes them a benign trusted entity in the classroom as safe as a teacher. **Google appears to be grooming our children to be socialised to their world** they are easy subjects for exploitation. Google's fast and loose approach to data normalises the children to devaluing their highly personal and valuable data. Preparing them to accept their life of digital serfdom.

Their logo with its kindergarten colours mis-directs users into believing they are a nice harmless company. Google trading as Alphabet, is The world's most powerful company, the US Congress is almost powerless over it. It was a defence contractor (Project Malvin) and the NSW Department gives them access to our children's data.
How does a US defence contractor pass a Working With Children Check in NSW?
How does a company that has run rough shod over harvesting and processing peoples and children's data around the world make it safe to handle our children's vulnerable identity?
What verification is there that ALL data is destroyed with all data contractors at the end of its purpose?

Google harvesting of location collection https://in.reuters.com/article/uk-australia-google-regulator/australian-regulator-initiates-court-action-against-google-idINKBN1X802D

Whist I requested the GSuite Enterprise terms and conditions, that our children are subjected to, from the NSW Department of Education, I still have not received it. It should be readily visible on the Department's website. I have noted in other Google education contracts that I have read early on in the T&C,s it says words to the effect that it does not use the data for targeted advertising but deeper in the T&C's it uses linguisticly dense language that insinuate that data may still be deep-data mined, a process that could easily de-anonymise data. I could see no commitment to data destruction once the data use has bee fulfilled. This data could also recreate psychometric identities of students. A process that could easily be used against them in 5, 10 or 50 years time.

Our Chief Scientist Alan Finkel says:
"But Google wants to do that - not for two weeks but potentially for the rest of your life. The idea of ***treating humans as objects****, as data, to be studied and manipulated, rather than as cherished individuals entitled to inherent worth and dignity, stirs our deepest convictions.*

Students Seen as Pavlovian Objects

Much of the software sold in education a uses Pavlovian rewards in a similar manner that the one arm bandits designed by gambling company's which uses similar respondent conditioning, such as empty electronic rewards, to hook their customers. It is well knows that many large internet company's cynically and cruelly use these techniques to entrap users. This respondent conditioning has two negative effects on students first it grooms them in to mis-beleving that, for them, electronic rewards / marks are important indicators of self-worth and secondly it offers pre-groomed minds into the hands of big data interests. Our children's minds are are a valuable resource for moulding and manipulating.

Industrial psychologists are exploiting every aspect of the human mind some are:

- Using empty electronic rewards, points and marks
- Bogus achievement and flattery (you have reached "Genius Level")
- The endless screen which makes it difficult to breakaway (Facebook, Twitter), (YouTube autoplay) creating addiction
- Anger motivation i.e. feeds of contentious material strategically juxtaposed with validation of data scraped ideals of user
- Manufactured social acceptability by creating an Ai managed environment or bubble uniquely designed to reinforce a unique tribal identity (with rejection of this ideal being a psychologically costly negative outcome). This is an early example of Ai abuse.
- Use of child like graphics to misdirect users that they are in a place that is as safe as a kindergarten, masking the reality that they are in the space of a large commercial concern whose primary responsibility is an ever increasing return to their shareholders

Many of these "tricks" are used in classroom software.
What chance do children have when big data interests are licking their lips at the opportunity being offered up to them, I cannot see how the Department is blind to this.

This relentless type of education removes internal self purpose and autonomous self motivation and inner pleasure and replaces it with a system where online image supersedes real world self image and a constant need for dopamine satisfying simplistic continuous electronic reward seeking.

This could be seriously damaging the health of our students. It could even in some instances have fatal consequences.

Educational Outcomes : Data Consumers and Addicts

My experience of the our education system is that it is producing data consumers. Not well rounded students that can negotiate the real-world as well meaningfully use data to be in control of new opportunities and as a healthy tool.

Re-identification of Anonymised Data.

The Department cannot claim to be unaware about re-identification of anonymised data.

Google is a prolific collector of data points, tracking and finger-printing users location, identity and interests. On school computers use does student finger printing, stealth tracking and search results in the browser regardless of being logged in or not come under the Department privacy agreement?

https://www.theguardian.com/australia-news/2020/mar/08/melbourne-professor-quits-after-health-department-pressures-her-over-data-breach

https://www.csoonline.com/article/3505644/telstra-on-defensive-as-reverse-engineering-of-medicare-data-highlights-healthcare-security-risks.html

Statistical Disclosure Control
Psychometrics and Discrimination

There is much research on this today. Google as a data hoarder with so many data points could re-identify student data today with deep data analysis and in 3 to 10 years any actor with access to the data benign or with ill intent could use Microsoft Azure or Amazon tools and many other software tools to chillingly create a psychometric picture of any NSW student.
For example online work such as story writing structure by a 7 year old child, when cross referenced with every other child's data in Google and other servers or even a one off data breach could be a psychometric predictor of behaviour that may be unfashionable to a hostile institution in say 30 years time. This could be used as a potential source of disadvantage or even a weapon and create prejudice against the grown up child.
Education should be for the self empowerment of a child not the collection of information to subjugate that child throughout their life.

In many universities I have perceived a presumed right and and arrogance when handling this sort of data where the researchers status of their paper or data lab trumps individual rights.
The early seeds of Cambridge Analytica began with benign university research.

Department officials work closely with the companies above and must be aware of these risks.
How is Statistical Disclosure Control across time, institutions and the increasing ease of de-anonymisation managed within the Department?

Whose Ai Philosophy.

Artificial intelligence implies intelligence. Intelligence by its very virtue must have perspective.
For AI in the classroom what auditing is there of the algorithms used in the classroom? How can you be assured that the values of Ayn Rand (a popular pseudo philosopher in Silicon Valley) is not buried deep in the Ai teaching as well as in the weightings in the marking of students work?

Ai Experimental Ethics - Children as Guinea Pigs.

Ai is being developed by Google and many other Department suppliers. Our children are experiments in these company s development of their products. It is not a mature technology therefore the use and analysis of this data is an experiment. Google's Ai and data experiments are not transparent. Are they subject to the Departments own Ethics Board?

Google declared future is Ai, but currently it has no Ethics Board and given the future power of Ai ethically Google is like a ship without a rudder. There is no clarity on how commercial Ai is manipulating our children's data.

Ai is at its gestation phase, its power and reach over humanity will be all encompassing. Giving Google and others our children's personal data now is negligent at best. It would be better to apply caution before Ai prejudges our children and has dominion over their lives.

Orphaned Data

Google whilst its future seems certain today, it could, just like US giants AT&T and RCA be broken up, or as data becomes more mature it could become just a commodity and be sold off to various data wholesalers in 5,10 or 50 years time. This threat is even bigger for for smaller companies who are subject to by-outs and maybe only just for their valuable data.

Perpetual Data Abuse.

The Department understands the very long-term risk of data misuse when it was involved with campaign on teenage sexting years ago the essence of the TVC was that once it is put out there it is always out there, so it understands risk of perpetual data abuse.

Human Rights

Many years ago I presented a paper that explored how just like in the New World when land was just acquired, today there is a similar parallel in the New Data World which has been created by companies like Google setting the rules as before there were none. Now companies like Google have strategically made their right to own our data the as the de-facto starting point and from their position of data dominance we are now struggling to reclaim human personality privacy rights of our children.

There is a power imbalance in our schools with data companies able to set the agenda.

We must ask: Do our children have a right to psychological privacy?

UN Universal Declaration of Human Rights Article 26. (2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms.

https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights_2019_DiscussionPaper.pdf

Jurisdiction

Google T&C's I read are subject to the Laws of California as well as to US Federal Laws and the secret United States Foreign Intelligence Surveillance Court. Our Australian School children seem to be subjected to the US Law.

Microsoft understands the importance of server sovereignty and in 2018 took a critical issue with Irish server sovereignty to the US Supreme Court, it was a major case.
A year ago I spoke with very senior Microsoft Australia personal who said that they used to have Australian sovereign servers however he sheepishly said they no longer have any.

What countries and jurisdictions is our education data stored and subjected to?

Data Sovereignty Case https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States

Turnitin Software a Mortal Threat

Turnitin is a very easy vector for the targeting of students that have fled oppression in their home country. In the appendix there is a scenario that I encountered where refugees and their family can be put at risk with lazy poor policy. This is a genuine HIRO risk. It was submitted to UTS in April 2018. Since then with regional tensions the risk has increased. See appendix.

Risk Assessment.

Is there a risk assessment and a Privacy Management Plan that looks forward 50 Years that the Department has done that examines the risks outlined in this letter and in the appendix? If so I would like to see it. It should be a public document. Therefore no need for a GIPA request.

Permission for use.

This is a public letter I give permission for it to be used 1,5,10 or 50 years time should it be necessary to clarify that the department should have been aware and understood the risks as a data handler of our children's very private, valuable and powerful data. Anything else would be negligent.

MP Paul Fletcher
About a year ago I expressed my concerns through my MP Paul Fletcher Minister of Cyber Safety a who kindly forward my concerns to your Office. I did receive nice personal but meaningless generic response. Hence this open letter

I would like **my children's data to be removed and destroyed** from all data handlers that they encountered during their schooling. They are European Union Citizens and under the GDPR they have an extraterritorial right to be forgotten I will follow this up in a further communication with your Data Controller. As they have finally graduated there **is no need to have any data, <u>of any type</u>, of them stored by any data contractors.**

These important issues are central to what education is about and who it is for. I look forward to a response to the issues above.

Sincerely Gerard Hosier

<u>APPENDIX</u>

This is the Safety hazard report submitted to UTS on the risk of political persecution with the use of the education tool Turnitin. It is also applicable to the NSW Department of Education.

Turnitin

HIRO: A health and safety hazard has been reported on your behalf. Date that the hazard was noticed: 04/04/2018

Date that the hazard was noticed: 04/04/2018

Description of the hazard: Defining the Hazard, Students, who have fled their homeland due to persecution, could have their safety and the lives of their families put at real mortal risk by the exposure of very personal assignments that are critical of the scenarios and power structures of the country's they have fled. The risk in many assignments at UTS students are encouraged to write essays on issues that are personal to them. In the classroom they believe they are working in a safe place with a personal relationship between a them and their lecturer. They write their essays believing their audience is a one on one with their lecturer. Upon submission their assignments are mined by an outside U.S. based contractor Turnitin for plagiarism. One of the features of Turnitin is that it allows lecturers from overseas universities to request to see the full text of a submitted assignment. How this happens in practice is the overseas lecture requests to see the full text, a pop up appears on a UTS screen with a yes or no button allowing the paper to be seen by the overseas lecturer or institution without authorisation from the student at risk. Is very easy to just click the yes button by a naïve lecturer who has not been given clear instructions from his institution of the risk. One of the issues with this risk is that it is a silent risk where the person receiving the information can pass it on and abuse that information against the student and their families putting them at potential mortal disadvantage with no audit trail.
Vectors: Potentially there are several ways that this could be exploited. An institution in the students former homeland may be a subscriber to Turnitin and submit a paper with extracts that a dissident would typically quote which, when data matched, with the students assignment would flag potential plagiarism and allow them to request to see the paper. It may also be possible for a sympathetic lecturer in a similar manner in an apparently safe country to request the original and pass it on. As a lecturer in a different institution I have come across a scenario like this that rang alarm bells.
The actions already taken to remove the hazard: <%HazardActionsTaken%>
The suggested additional actions required to remove the hazard: <%HazardRecommendation %>…

A redacted copy of an email I received
*Dear ****

*Turnitin is forwarding this request on behalf of X Y Z, an instructor at University of * . This instructor requests your permission to view the paper, "Name of Paper (which has the student name & Student number in the header) ", submitted to your XXXXXXXX class at 123 Institution*

This instructor has found a 8% match to this paper in a paper submitted to his or her XYZ class.

If you chose to grant permission to the instructor to view the paper, simply reply to this email. Please confirm the text of the student's paper is displayed in your reply email. By replying to this email, you will be sending an email (including the text of your student's paper) to the requesting instructor, X Y Z.