Forum Privatheit keynote -- November 21, 2019, Berlin
defenddigitalme

(Slide 1, title)
On the 30th anniversary of the opening of the UN Convention on the Rights of the Child, I invite you to start today, by listening to young people in their own voices.

In the summer of 2019, we, defenddigitalme, worked with the Warren Youth Group in Hull, North England together, the organization Designing for Children's Rights (D4CR), UNICEF and Hiidenkivi High School in Finland to produce a short film to challenge decision makers and companies about current data practices. Here's what they had to say.

[Play trailer] https://youtu.be/8BzyOmkXJIA

(Slide 2)
Every child in the world has a right to grow up healthy and safe, to develop their potential, to be heard and to be taken seriously. The UN General Assembly enshrined these rights thirty years ago in the Convention on the Rights of the Child. The full range of human rights enshrined in the Convention should be fully respected, protected and fulfilled. The right to education itself, the right to be heard, and the focus of this hour, the right to free and full development. These are protected by the right to privacy.

No one may engage in arbitrary or unlawful interference with the child's privacy, family, his home or his correspondence or unlawful attacks on his honor and his reputation. The child has the right to the protection of the law against such interference or attacks.

But what does this rights mean in practice for education, if political decision makers welcome software with high praise, that does not respect that right?

If schools impose software that monitors everything a child writes on a computer screen, matched and profiles use against secret keyword libraries with thousands of words in selected languages to detect signs of radicalization, risks that the child is facing to themselves or for others; to unspoken thoughts of activism or to recognize extremism?

A leading UK company is currently using a case study it claims comes from a UK school, in its advertising materials, identifying the schoool where a seventeen-year-old girl who was writing about her rape in a letter to her mother, that was first identified by the company who communicated it to the school.

What does unlawful interference in a child's privacy, family and his home, if this kind of software is imposed on every child through new mobile phone contracts? The British newspaper, "The Telegraph" reported in August that a British company has reached such an agreement with the German federal government to make their surveillance app available on thousands of children's mobile phones.

What do consent, and the right to be heard of Article 12 mean, when children have no other choice than to be in compulsory school? The system demands their daily interactions with hundreds of companies and their business groups. Children and parents cannot freely

choose or refuse to invite them into the life of their child and will often not know as a result, who tracks their behavior, profile or predicts their future performance; or who might be responsible for deciding what part of the curriculum your child is doing next, or not. What do the rights of the child mean if we do not respect them?

I would like to ask you to be the advocates who our children need so that they can lead their lives to the best of their ability, and can thrive into adulthood.

Yes, they need protection, which is talked about very often, and they also need the defense of their participation rights. And they need privacy.

I am the founder of defend digital me, a call to action to protect the rights of children to privacy. We are teachers and parents who are looking for safe, fair and transparent data processing in education, in England and beyond. The campaign is sponsored by the nonprofit organization Joseph Rowntree Reform Trust Limited.

In 2017, the English Children's Commissioner published a report entitled 'Growing Up Digital' and came to the conclusion that we are failing in our basic responsibility as adults to give children the tools to be agents of their own lives.

If the issue of managing our privacy is difficult for adults, it is even harder for children. Since one third of all Internet users are children, this is an urgent question.

For children, we need to address some of these urgent data management issues, to solve autonomy and the right to privacy now. We have to prevent the known harm children suffer today. And we have to be forward thinking, considering all of society, and the future of our state education systems over the next twenty years. And how we want to shape them together.

Children cannot put growing up on pause, while policy makers sort things out.

And while governments do little, companies are not only gaining ground, about what is done today, but also control the direction of travel. On privacy. On ethics. And they build the limitations, of today, and into the future, of what is possible.

(Slide 3)
"Education happens to be today, the world’s most data-mineable industry by far," said the then CEO of Knewton, José Ferreira, in 2012, seven years ago.

In the meantime, millions of children started school. Have changed school changed. Left school. And they have no idea where their digital footprints have gone, in the educational landscape and in the world. No idea who knows what about them or how these data can be used in the future by third parties.

But why, one might ask, is this such a big thing for education? We have long had data protection law, and we have an updated privacy law in the framework of the GDPR. (DSGVO).

(Slide 4)
In 2017, the International Working Group on Data Protection in Telecommunications, the so-called Berliner Gruppe, recognised in its working paper on e-learning platforms, that, "The sensitivity of digitized pupil and student data should not be underestimated".

Most people have no idea what a day in the life of a child in education looks like. Well, here it is. An imaginary day, based on the life of one typical 11 year olds in England. Your own school day may look very different.

(Slide 5)
But let's take a look, because the core activities in many educational systems are similar, from Harari to Hannover. From Helsinki to Hong Kong. On the iPad, on Chrome Books or on your own cell phone, children interact on a daily basis with hundreds of digital providers.

Each of the activities at the centre of this day I describe in this data wheel, are the core activities of data processing in a school.

Admissions system. Attendance and absence. Assessment. Behaviour management. Benchmarking between teachers, classes, schools, or the regions. Communications between school and home. Managing health and safety, human resources and staff, special educational needs, safeguarding, And that is all before most learning, lesson and homework delivery, timetables and IT administration.

And for a child all of that may touch them in a day through data that goes into, across and out of a core school information management system. That is data generated about them, not with them.

On top of that, add in all their own daily interactions.

- 07:30 At seven thirty a message arrives on Maria’s and her parents’ phone to remind them of a special event today.
- 08:30 At eight thirty she is walking across the patrol crossing and filmed on the safety officer’s bodycam before showing up three times on the school entrance and playground CCTV as she walks toward her first tutor lesson.
- 09:00 By nine o’ clock she has been registered on the school information management system as present, and goes to her first lesson.
- 09:15 By nine fifteen she has logged onto Google classroom, and silently the school web monitoring software starts up, matching every search term against a set of thousands of keywords that will trigger a system alert if found. Self harm. Mental health. Bullying. Stranger-danger. Terrorism. Her quick search for cliffs from the family walk she enjoyed that weekend, triggers a flag for potential suicide risk.
- 10:00 At ten o’clock she’s asked to use a maths app on her own phone, a quick quiz to end the lesson. She enters her username and school email address and data of birth as verification. The teacher sees everyone’s scores and progress on bar charts

on their own screen. Everyone who still hasn't logged in, is assigned a negative behaviour point, on the classroom behavioural scoring app.

- 11:00 Eleven o'clock and in science, Maria is logging into the new Ai led platform, watches a short film about gravity. She wasn't paying attention only gets nine out of ten on the multiple quiz choice: Watch it again, suggests the machine learning app, having recorded her mouse movements every two seconds. She cannot proceed to the next chapter without it.
- 12:00 She races out of the classroom as soon as the bell goes to be first in the lunch queue. Washing her hands just wastes time. At the front of the line for the cashless lunch she pushes her thumb into the machine to read her biometrics for the tenth time that week. Like Maria, every child in the long line behind her they must use it to only to buy lunch, but to borrow a library book.
- Before they leave school that afternoon, they will have logged into three more apps, including the foreign language app matching vocabulary to pictures, and the Reading app to measure the number of words they've progressed in their reading that week, and have to see the librarian if the profile over that month shows slowdown. The Google classroom platform will have their homework tasks and contents loaded up to download at home.
- At the after school football club their attendance is checked against their names from the school information management system provided details. Their sports changing space recorded on CCTV. Their team photo taken for the school website, social media pages, and local newspaper for the tournament news that weekend. Maria feels left out as she's the only one whose parents have said no to use of their photographs for marketing.
- 17:00 Crossing back across the playground again on CCTV three times, she uses her photo bus pass to get on the school bus, and get home.
- 18:00 At six o'clock, she logs back into Google classroom, uploads her homework, watches some YouTube video on gravity, maybe she finds it interesting after all, and all the time the web monitoring watching for signs of suicide. She's on a watch list now since this morning's system error. She just doesn't know it.
- 22:00 At the end of each day, the school information management system sends changes and new data to the regional authority database to match with welfare, health, policing records and build predictive profiles for interventions.
- Once a term, three times a year, it is all sent to the national database in the school census, where it grows in the National Pupil Database, now standing at over 21 million people in England, with a lifetime of education and sensitive data from age two to nineteen, so that government can benchmark your school's achievement, and later, joining the school records with university records your first employment earnings and or state welfare payments, they will determine how much our education cost the state and suggest it tells you which courses have the greatest economic return.

Maria doesn't know that yet of course. She's eleven. Her data are building the database about her that she will never see. Never have a chance to correct that error. Never know how much she may be shaping the state policy built on little more than a variety of teacher opinions and tests that measure little more than the picture of one day.

That is a fiction, but very close to my own daughter's everyday reality.

(Slide 7)

> “Children do not lose their human rights by virtue of passing through the school gates.” UN Committee on the Rights of the Child. The aims of education (2001).

But the reality is that their rights are not even left at the school gate, they have been removed from her 24/7, 365 days a year by the state and the English school system. Schools are the gatekeepers not only for the State, but for thousands of third parties to gain access to millions of children’s lives.

(Slide 8)
We are also processing extremely sensitive data. In addition to data protection law, there is a requirement to ask for active consent to capture a child’s biometrics in schools in England and Wales, under the Protection of Freedoms Act 2012, though it does not apply equally to children in Scotland and Northern Ireland.

Despite this, the collection of consent fails.

We carried out a survey through Survation, in February 2018, of one thousand and four parents of children aged five to eighteen, in the state education system.

We asked them if they knew what systems their child used in school? One quarter said they have no idea. Nearly 80 per cent had never heard of the national pupil database.

(Slide 9)
Thirty-eight percent of those whose school uses a biometric system had not been asked for approval.

My co-director, Pippa King, started her own campaign almost ten years ago, Biometrics-in-Schools, as the school almost gives their little sons their fingerprints without their knowledge and permission. When she asked the Headteacher why, they said, we do not have to ask for approval. As a result, and after the work of many campaigners, new law was introduced in 2012, but it still fails in practice, because in practice there was no management of the changes. Zero training.

We declined this year for my ten year old. She went to big school. We had a conversation before hand with her, why we had chosen not to use the fingerprint system and how the alternative card worked instead. She understood and was happy to do this. The same as her older sister. Week one, the school lined up every child in the new year group. They were fingerprinted one by one, including my daughter, because she was too polite and timid to tell her teacher, they had made a mistake.

Children’s rights at left at the door.

(Slide 10)
Consent does not work when behaviour is monitored and school staff choose to record it using an app that makes sounds for good or bad points, to praise or shame a child in front of their peers. The idea that stigma and shame are beneficial is problematic.

Even more clearly, if the teacher projects the whole class screen on the wall at the front of the room for the lesson.

Not only is Big Brother watching you, but your peer group. And the company, and their global company group partners. And their new owners, a U.S based private equity company.

(Slide 11)
Not only apps can be used to surveill whole class behaviour, but cameras too and how do you respect individual rights when policies affect the whole class?

This education trade magazine, Schools Week, reported this summer on a school in Birmingham that has installed cameras the size of a fifty pence, or a two euro piece. They monitor voice and movement as well as record film.

Gait analysis, will be the next big thing the company CEO has told me.

So where should the boundary be of being told what to do and having to accept it, conform or have no place at the school, with the rights of the child to education, and fairness when it comes to edTech policies?

Consent does not work for children in school.

(Slide 12)

Where does a school's right to determine which apps, platforms and policies it chooses, fit with the children's right to privacy, and to be free from exploitation?

Apps that monitor children's behaviour points may have strong terms and conditions about not reselling children's data. But they might also require that the school accepts click wrap agreements -- pre-packaged agreements designed by the company that cannot be changed by the school but have to be accepted or don't use the product --- and those agreements may include the use by the company of the parents' and child's email address to be able to send them additional content, to advertise that content and premium services perhaps even based on the child's behavioural history that the app has collected, or the location of the family based on the phone IP address. Or the cashless payment company may simply use the design of its home page to deliver a massive advert to the captive audience of parents to market its own daughter company, a child's online pocket management app.

Or we could take a look at a whole range of apps and platforms terms and conditions that commonly say, the school consents on behalf of the child, to the anonymisation of their data for data analytics and product improvement and further purposes in perpetuity.

And then consider that it is impossible for a school to really understand how many of these apps work. I was speaking with a colleague yesterday, from the Oxford University of Computer Science, Jun Zhao, worked with others on the assessment of nearly one million apps. Neary ninety percent of them were sending data to Google because of the analytics built in by design. And the developers might not even know the full extent of what their code does, when they borrow bits of design from other people's code, from code libraries, -- a bit like borrowing lego bricks from another model to make your own bigger and better -- and they might not fully understand what the implications are for their own end product. How can teachers be expected to understand all this and explain it to families?

On privacy. On ethics. On data minimisation. Consent does not work for children in school.

(Slide 13)
This manufactured consent is meaningless to children and families that must agree when the child starts school by signing a home school agreement. That provides consent to the invasive web monitoring programs that run in English state schools, that may monitor --depending on the company--, at home, may monitor your personal mobile phone behaviours, may take a webcam photograph on triggering the keyword, may create data that are used in a referral to the anti-terror Prevent programme, that may send sensitive personal data to the U.S. or be now processed by a Bahraini owned multinational corporate. That consent is to processing is being collected in a single sentence of fourteen words.

“I understand that the school monitors the use of digital technologies by all users.”

(Slide 14)

> “The price of innovation does not need to be the erosion of fundamental privacy rights.” (Elizabeth Denham, ICO, 3 July 2017, findings on Google DeepMind and Royal Free Hospital unlawful processing of health data for the company’s product development)

(Slide 15)
What happens then, if we all agree, there is insufficient legal basis for data processing for these kinds of invasive practices, and regulators do their job and enforce? What difference does that make?

(Slide 16)
Let’s look at the recent case studies of Facial Recognition in schools. First in Sweden.

The Swedish Data Protection Authority argued this summer, that consent can not be applied since students and their guardians cannot freely decide if they/their children want to be monitored for attendance purposes.

When examining if the school board can rely on any of the exemptions listed in Art. 9 (2), the supervisory authority found that this was not the case.

The found that facial recognition processing activity was one with high risks since new technology was used to process sensitive personal data concerning children.

And in the view of the authority, the school board was not able to demonstrate compliance with Art. 35 GDPR and that the school board was required to consult the authority in accordance with Art. 36 (1) GDPR.

This was unlawful, despite the fact that the systems were not Internet connected, devices reportedly secure, and that importantly, families were asked for consent.

The vital finding, the only one that can protect children’s rights in these circumstances given the deep power imbalance between the school and the child or their family, is that consent is not valid in such an educational setting.

(Slide 17)

The CNIL in France has followed suit, saying that the schools in the south of France demonstrated a failure of fundamental principles of data minimisation, proportionality and necessity. A vital decision not only for school children, but for everyone, given that their government intends facial recognition to be used nationwide on the streets, which I implore you to revolt against with all your might.

Facial recognition has no respect for anyone's "private and family life, his home and his correspondence, even if subject to certain restrictions that are "in accordance with law" because everyone, without choice is subjected to it.

The principle of "necessary in a democratic society" means a right to be free from interference and that interference may be invisible but its chilling effect will be felt most on communities already disproportionately under surveillance by the state -- people of colour, foreigners, gypsies and travellers, women and children.

(Slide 18)
Where else has regulatory enforcement begun? In Norway, it was insufficient technical and organisational measures to ensure information security in a home school communications app. And there are plenty more of those kinds of apps.

So it can make a difference, but so far, only in individual school cases, not across the sector.

(Slide 19)
So much for the effects on individuals and collective rights.

What about the impact on the collective public good and commercial profit?

For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the global edTech market, propagated not only by angel investors and tech accelerators in US and UK English language markets, but across the world. Estimations of market value and investments range widely, from $8bn as noted in a UNICEF paper on rights and participation, privacy and right to reputation, to research from Metaari, 'The 2018 Global Learning Technology Investment Patterns: The Rise of the Edtech Unicorns', that suggested that Chinese edtech companies were the majority recipients of global edtech investment in 2018, snapping up 44.1% of a total $16.34bn market spend.

At the same time, under the global pressures to deliver low-cost state education, and marketisation, the infrastructure used to deliver state education and the children in it, are exposed to commercial 'freeware', software that companies offer at no cost, often in a non-explicit exchange for data.

(Slide 20)

Natasha Singer writing in the New York Times in May 2017, described how Google took over the classroom.

> "In the space of just five years, Google has helped upend the sales methods companies use to place their products in classrooms. It has enlisted teachers and administrators to promote Google's products to other schools. It has directly reached out to educators to test its products — effectively bypassing senior district officials.

> And it has outmaneuvered Apple and Microsoft with a powerful combination of low-cost laptops, called Chromebooks, and free classroom apps.
>
> Today, more than half the nation's primary- and secondary-school students — more than 30 million children — use Google education apps like Gmail and Docs, the company said. And Chromebooks, Google-powered laptops that initially struggled to find a purpose, are now a powerhouse in America's schools. Today they account for more than half the mobile devices shipped to schools."

You capture staff training, you capture the structure of the curriculum and the route to deliver it. You capture the procurement by evading it with freeware. You capture the delivery and the physical infrastructure and platforms upon which the education system is delivered to millions of children you build yourself a gateway to control of the education system in a whole country. And then you copy it across countries across the world.

Google knows what content teachers create, and they have the capability to know how long a child takes to read it.

Google is driving a philosophical change in not only the delivery of state delivered education but its purpose— prioritizing training children in skills like teamwork and problem-solving while de-emphasizing the teaching of traditional academic knowledge.

Why focus on knowledge after all, if your company has turned its search term to looks for knowledge online, into the action of doing so? Google has turned its company name, into a verb.

In English, teachers and children alike, will say, "I don't know the answer to that, but I can Google it, to find out."

If you are only catching up to this now, it is not too late, but you must act to ringfence the purpose of public schools. Is it to create knowledgeable citizens, with a capacity for and love of learning, to allow the full and free development into adulthood or is the central purpose to produce digitally skilled consumers who only know how to live with Google at the centre of your everyday, and for life?

The skill sets are not mutually exclusive or a zero sum game, but who decides what the rules are?

(Slide 21)

Right now, the decision makers are the developers and company owners shaping what apps content look like, how far they are permitted to do to nudge a child's behaviour, how do they affect a child's mental health, how they shape the personalised curriculum, how they judge a child's performance, how they judge a child's Internet search intent, and what adverts they show or data analytics they collect and process -- all these decisions are dependent on companies that are subject to change of control at no notice, through sales, mergers, private equity and takeovers.

The numbers of actors involved in the everyday data processing in a child's day, year, and lifetime is very hard to visualise, due to their large volume.

For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the global edTech market, propagated not only by angel investors and tech accelerators in US and UK English language markets, but across the world.

Estimations of market value and investments range widely, from $8bn to research from Metaari, ‘The 2018 Global Learning Technology Investment Patterns: The Rise of the Edtech Unicorns’, that suggested that Chinese edtech companies were the majority recipients of global edtech investment in 2018, snapping up 44.1% of a total $16.34bn market spend.

At the same time, under the global pressures to deliver low-cost state education, and marketisation, the infrastructure used to deliver state education and the children in it, are exposed to commercial ‘freeware’, software that companies offer at no cost, often in a non-explicit exchange for data.

Insufficient training and change management often accompanies the introduction of new technologies, with insufficient learning materials and under-qualified teachers when it comes to assessing tools on the question of data processing.

(Slide 22)
In an experiment in the City of Espoo, Finland, in cooperation with the company Tieto, Artificial Intelligence was applied to analyse health and social care data linked with early years education from 2002 -2016. (Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch 2019)

The predictive nature of such surveillance applied to early interventions could have significant impact and inadvertent consequences from an early age.

Yet we don’t even know often if these products work, except from the company’s own marketing.

"What is meant when organisations apply ‘AI’ to a problem is often indistinguishable from the application of computing, statistics, or even evidence. The usage of the phrase has become so laughably ambiguous and general, it is almost like saying that to solve an urban infrastructure problem, one must ‘apply power tools’…(Michaeal Veale, UCL, London 2019)

Artificial intelligence can also be used for low level decision making, such as assigning class seating plans based on the recording of children’s behaviour data, analysed in opaque ways to determine room layouts optimised for behaviour.

The scale, speed and simplicity of data transfer has been exponential since the creation of the Internet and world wide web, while data storage cost has fallen. The barriers to data access, copying and distribution have been diminished through easier accessibility, and with it the protections offered to data subjects in practical terms, have failed to be respected by companies and institutions.

The potential global implications for the security and stability of the state sector education infrastructures, the personal costs to children in terms of privacy, and effects of habitualisation and normalisation, may last a lifetime for this datafied generation.

How do we build a rights respecting environment for life?

(Slide 23)
Because what is next? The next generation of technologies are already messing with the next generation of children in ways that we do not understand.

We are failing to ask the right questions of policy makers and companies.

(Slide 24)
In 2013, when our then UK Education Minister Gove and his Department for Education advisor Dominic Cummings were talking about social mobility and genetics, and Boris Johnson wrote about it in the press, the geneticist Professor Plomin was invited to the Education Select Committee to talk about the underachievement of white working class boys. Some take the proposed implications for education, very seriously.

Brain scanning tools. Social, emotional behavioural detection. Thought control and genetics. This is not the stuff of science fiction but already in some of our children's classrooms, and with the aim of altering our children's minds and behaviour.

The work of Ben Williamson of Edinburgh, questions this, and is something you must look out for and read if it is an area of interest.

In the face of these advances in the volume and velocity of data collection and transfer, and the next level of technologies already with access to children in the classroom in trials, there is an urgent need for regulation to support rights in practical and meaningful ways. And while some things should simply be regarded as too invasive to use, we must make sure it is not too narrowly technology specific since the new thing will be just up ahead.

Lawmaking and procurement at all levels of government must respect the UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.

> *"a State should not engage in, support or condone abuses of children's rights when it has a business role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties. States should not invest public finances and other resources in business activities that violate children's rights."*

The changing landscape of what is permissible, what is possible, and what is acceptable in education is being tested on our children.

For companies,three years to trial and bring a product to market, or to discover the efficacy or pedagogy of an edTech tool is or is not working well, could be a short time, but it could be more than a quarter of a child's lifetime in compulsory education.

There is little requirement in procurement, to find what is pedagogically sound and what is developmentally appropriate, it is not part of overall edTech risk assessment.

Assessment of risk in data processing is not a one time risk at the start of data collection, but is spread across the life cycle of data processing. Indeed some of the most significant risks may be delayed to discover only in the future adult, or be in how it changes behaviour. That

should be reflected in the assessment carried out, and the information given to children and families as a result, at the start, during, and at the end of their personal data processing. This would increase informed processing and raise controllers awareness of their accountability role and for risk.

Some are keen that Data Protection Impact Assessments about children must be tailored to them. For example, the Danish Institute for Human Rights, as they wrote in 2016, and yet these assessment must also adequately explain passive data collections and risk. Invisible information about a child whilst in school (RFID, beacons, virtual assistants in the classroom and Internet Connected Things) can create a vast digital footprint that neither the family nor child nor even the teacher may have actively provided.

Arguably risk assessments should be thorough and technical documents with summary explanations of functionality and risk that can be extrapolated into lay terms. Data impact assessments must become routinely integrated into procurement processes.

Adequate data protection, privacy and ethical impact assessment must become embedded in the introduction of any technology and require appropriate levels of knowledge and training. But it cannot be left to individual schools and teachers to do this adequately.

(Slide 25)
Consent and contract terms must be rethought in the context of education.

(Slide 26)
Only by reshaping the whole process, will we have any chance of meaningful policies that restore the power balance to schools and to families, and restore schools to a strong position of data controllers and delegate companies to data processors with much stronger controls than today, on what they are permitted to do in terms of data processing and trial and product development. That infrastructure may not exist, but we need to build it.

This is a case study of how it is done in the U.S. governed by FERPA law. It is imperfect and still results in too many privacy invasions, but it offers a regional model of expertise for schools to rely on, and strong contractual agreements of what is permitted for processing. Schools are data controllers and processors cannot change terms and conditions mid way through the year, without agreed processes for notification and reasonable terms of change or to end the use of the product. Families get a list at the start of each school year (or every start with school moves) to explain all the companies their child will be using. They consider this consent, which it is not, it is simply acknowledgement -- but crucially in addition parents retain the right to object, and schools are obliged to offer an equal level of provision via an alternative method, so that objection is not to the detriment of the child. What I would want to see as well, is end of year reports, to say this is what we actually did. The model is imperfect, but we could build on this and do better.

(Slide 27)
We can also do simpler things first. Such as standards and expectations on data security using statutory Codes of Practice. (Art. 40 GDPR / DSGVO).

(Slide 28)

The direction of travel advocated for by Pearson and other companies, including the EdTech community and govt multi million funded hothouses to find evidence of the value of edTech — is accompanied by the cry for more data, on every child, at all times.

Put all these things together and get them wrong: poor data based on opinions and bias, unethical applications and uses by third-parties, and using these data at scale for Machine Learning and AI, prediction, punitive uses of population wide data without transparent oversight and access by the individuals, increasing the volume of data collected and lowering the age at which we do — we are going in the wrong direction.

And we are already seeing push back from parents. Most recently from China on brain scanning headbands. Growing awareness of data misuse will lead to a growing number of data collection boycotts, such as that led by Against Borders for Children (UK) (2016-2018) against nationality data as a result of pupil data use in immigration enforcement. Or look at the Parent Coalition for Student Privacy, (US), that shut down Bill Gates plans for InBloom, in 2012-14.

When the U.S. online Summit Learning program imposed Silicon Valley, commercial tech-centric models into public education in Kansas in 2019, there was fierce pushback from parents.

If this generation is not to be held back by the data burdens of their past, but should have the freedoms needed to shape it, then children must be able to exercise their rights in education in a way that is not detrimental to their own and their collective future.

Where does this mean that we need to change, to restore the balance of power back to schools and to what families expect from the school? It would need to be radical across the whole process.

This involves changing current practices on

- Reducing the investigative burden,
- Children's agency,
- The role of families,
- The role of school staff,
- A model management framework not consent,
- Procurement,
- Automated decisions, profiling, and AI,
- Horizon scanning on new technology,
- The permanent single record,
- Representation and remedy,
- And lifetime accountability for the data cycle.

(Slide 29)

The public climate towards commercial exploitation is changing, as awareness has grown for example of Facebook data misuse, and the tolerance for interferences with our privacy rights is diminishing. The public expects better. The only reason we have not yet seen more backlash in schools, is I believe lack of awareness. But when that comes, we need to be

able to offer a better alternative. Our children should be able to expect more from us adults, if we are to give them the tools to be the agents of their own lives.

Since we are celebrating the rights of the child here, in thirty years of the UNCRC, I would like to use the words of a child to conclude, and borrow the words of Greta Thunberg at the UN climate summit in New York, from September 2019. She talked about the climate outside, but I think it is just as good a fit for the environment on their data processing.

The eyes of all future generations are focused on us, the adults. And If we decide to let the children down, I say - they will never forgive us.

The time to act is now.