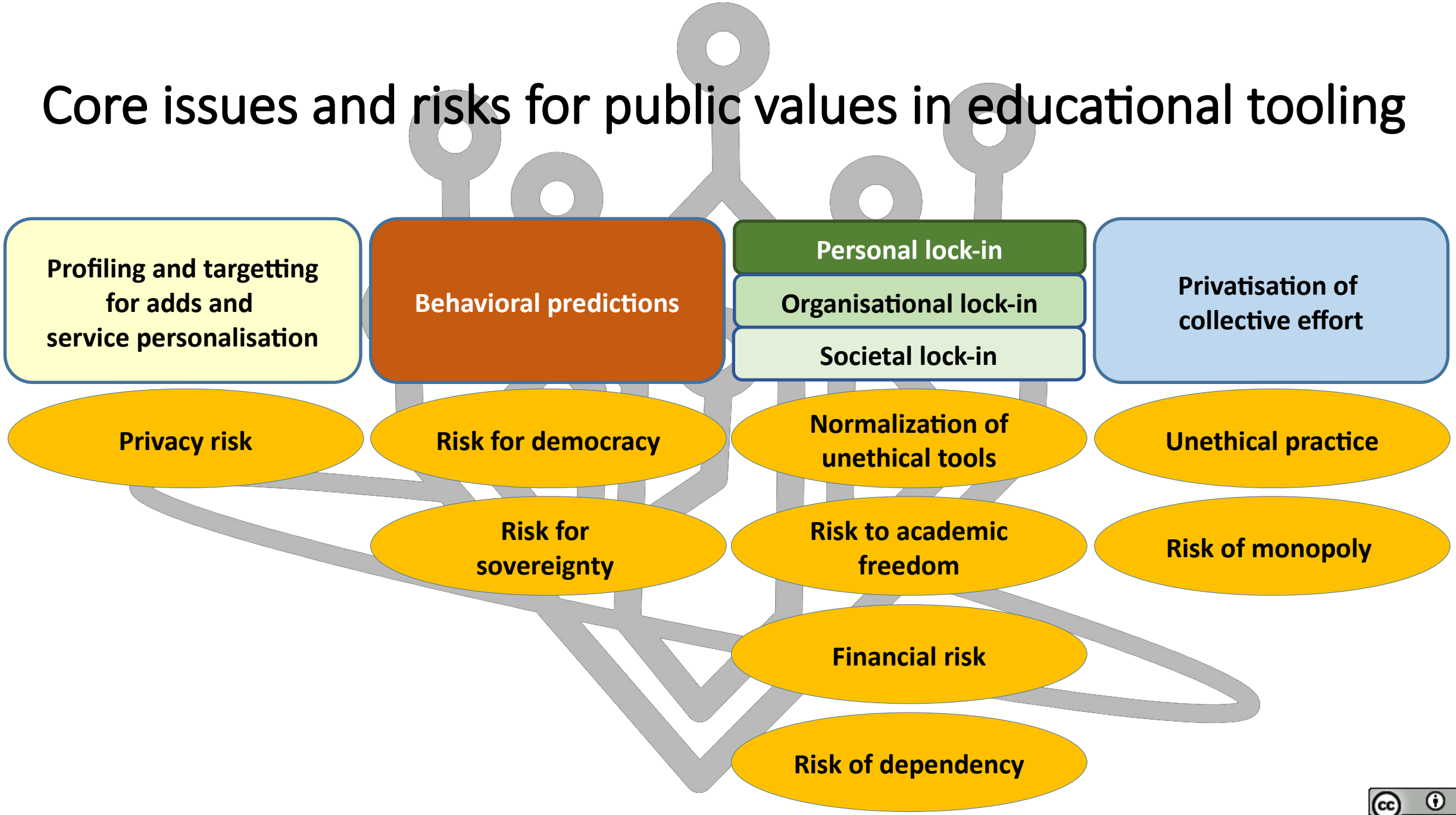
Core issues and risks for public values in educational tooling



Profiling and targetting for adds and service personalisation

Privacy risk

Issues	Explanation/ example
Data is combined from many sources.	- Data is combined with datasets from main Google services like Gmail/docs. - Data is combined with datasets from 3th parties. - Data is combined with datasets from basic "free" tools. For example Google offers tools that are very easy for developers, but the actuale purpose is data collection. *(Fonts, Firebase, analytics, DNS, templates, etc.)*
Data in cloud services is routinely scanned for content that violates terms of service, risking a block of the account, also for false positives	This is broad dragnet surveillance, executed by private companies, mixing law enforcement and protection of business interests. Search should only take place when there is a cause and a warrant for it, not always and systematically.
Service personalisation is intransparrent. Often there is no opt-out.	Even if users are aware that personalization is happening, there is no way to figure out how and why. Example, YouTube recommendations and results from search engines are presented as neutral results. In reality results and recommendations are optimized to serve business interests. The user cannot switch of personalisation.
If data is not traceable to a person, data is no longer considered 'personal data' thus the AVG does not apply.	

Behavioral predictions

Risk for democracy

Risk for sovereignty

Issues

Explanation/ example

When using surveillance capitalist services you must provide data to "improve our services".
What is meant by that is your (meta)data will be used to train AI algorithms in which you have no say.

Facebook (no accountability nor transparency in how they let collected data be (mis)used by third parties) leading to the Cambridge Analitics scandal (**abuse of** Facebook **data for propaganda**).

Microsoft and Google, personalising services without transparency nor accountability while, presenting themselves as "neutral" services, eg on Youtube, leading to **radicalisation** and **polarisation** by algorithmic recommendation of next video clip, sending people "down the rabit hole".

Personal lock-in

Risk of dependency

Normalization of unethical tools

Issues	Explanation/ example
Migration is made difficult.	You invest time and energy in figuring out how to do things, adding your data, building your network, if you move away you loose this investment.
Non-compatible with competing products.	The user is dependent on the features the vendor is inclined to offer. Supplier of those "free" services may decide to terminate the service any time. See *https://en.wikipedia.org/wiki/Category:Discontinued_Google_services*
Bundling of products.	For example, if you start using Microsoft 365 you get the whole package, incl. MS Teams integrated, setting competitors at a disadvantage.
Blocking of accounts.	When an inappropriate picture is found in MS Onedrive or Google Drive, you risk losing you entire Microsoft or Google account, so no access to O365, e-mail, Teams, Xbox, games and even your PC, or G-Drive/mail/meet, Youtube etc and even your phone. For example a case of the user ending medical pictures and of a user receiving unwanted porn pictures. *https://tweakers.net/reviews/9094/account-geblokkeerd-wat-nu.html*

Organisational lock-in

Financial risk

Issues	Explanation/ example
Migration is made difficult.	Open standards are ignored, so switching to an alternative comes with huge migration costs. As soon as exit cost are extreem due to becoming locked in, licence cost go up, often to extreme levels.
Bundling of products.	If your organisation has licences for Microsoft 365 you get the whole package, incl. MS Teams integrated, setting competitor at a disadvantage. So why invest in a Jitsi or BigBlueButton server?
Non-compatible with competing products.	The user is dependent on the features the vendor is inclined to offer. *(vendor lock-in)* *https://en.wikipedia.org/wiki/Category:Discontinued_Google_services*

Societal lock-in

Normalisation of unethical tools

Risk to academic freedom

Issues	Explanation/ example
Even if an institute properly did al the GDPR homework, with DPIA, proper implementation and a data processing agreement with lots of nice promises (even then CLOUD -act still applies) al the GDPR guaranties ONLY apply to the tools used at school or university.	It is not realistic to expect that students as soon they want to do something themselves (outside university) read the EULA, study the GDPR, conclude that their private accounts come with lots of privacy violations, and then start using something completely different, while university has taught them that these kind of surveillance products are OK. Otherwise they would not teach these kind of services, right?
With using cloud services of USA-companies, export restrictions that are result of USA politics get **influence over what universities can discuss or research**. This applies to any conversation, video, document or research data processed by a USA cloud provider.	Most well known example of this is Zoom cancelling an academic debate: *https://theintercept.com/2020/11/14/zoom-censorship-leila-khaled-palestine/*

Privatisation of collective effort

Unethical practise

Risk of monopoly

Issues	Explanation/ example
Millions of people contribute their corrections and suggestions to suppliers, mostly without being aware of this. (Somewhere deep in the EULA or data processing agreement is "your data may be used to improve our services".)	Google/Bing translate, and the spellings checkers of Google and Microsoft work really well, this is because millions of people contributed their corrections and suggestions to them, mostly without consenting to this use.
The first party that conquers the market can collect the most data, and can thus create a monopoly. As soon as market dominance is achieved, licence prices will sky rocket.	Due to the **network effect** the dominant party is almost impossible to catch up with. Schools, meanwhile, have become dependent and will swallow the price increases.
Proprietary adaptive learning systems not only teach students, also the student is teaching the adaptive system. This is a form of labor that mainly benefits the dominant market player.	Example "rekentuin" uses a ranking system for both students and questions. When a student answers a question wrong, the difficulty rank of the question goes up. Most schools and students are not aware and are not compensated for this free labor they are providing. The results of this collective effort belong in the public domain!

How to restore public values in educational tooling?

Above all:

It matters what you teach!

If you teach unfree surveillance services, that is what you will get:

A surveillance society, ruled by BigTech

By design:
- **-Privacy**
- **-Public Values**
- **-Ethics**

It all starts with the design. Do the tools you choose strengthen the core value's that your school or institution stands for? Choose ethical tools!

Data ownership

Schools an institutions should recognise the value of data. Data created by pupils and students is not theirs to sell

Open standards

Use services build on open standards, that allow you to leave with all of you data, and network relations.
Like: Mastodon on the fediverse

Free, open source software

Chose ethical and opensource tools, that an organisation can also selfhost. *Like Jitsi, BigBlueBotton or NextcloudTalk*

Attribute cost for lock-in: "**polluter pays**"

Cost for an exit strategy should be attributed to the party that created the lock-in, not to the service that an organisation is migrating to.

Teach ethical and open source tools

Since it really matters what tools you teach students or pupils, the tools taught in school will also be used and after college or school. Even if you can force BigTech to act GDPR compliant in school, it's unethical to teach those services if those terms are out of reach out of school.

Strengthen the public domain!

When we with millions of people collectively train an algorithm, the result of this should be in the public domain, thus use open source algorithms and open data sets.