Public Education, Platformization and Cooperative Responsibility: The Case of the Privacy Covenant in the Netherlands

Marco Houben, Jo Pierson

Public education, platformization and cooperative responsibility: the case of the Privacy Covenant in the Netherlands

Marco Houben[1][0000-0003-2011-2248] and Jo Pierson[2][0000-0002-9077-6229]

[1] imec-SMIT-Vrije Universiteit Brussel, Pleinlaan 9, 1050 Brussels, Belgium, marco.houben@vub.be, [2] imec-SMIT-Vrije Universiteit Brussel, Belgium

Abstract. Platformization increasingly changes educational pedagogies, policies, governance, financing, and the role of teachers in public education. As such, platforms start to play a vital role in the realization of the values and societal goals of public education. Platform governance typically focuses on the responsibility of one actor. Cooperative responsibility argues that instead, platform governance should be the result of the dynamic interaction and allocation of responsibilities between platforms and users, supported by a legal and policy framework created by state institutions. Qualitative interviews into the construction of the Privacy Covenant for public education in the Netherlands are used as a case to investigate cooperative responsibility 'on the ground'. The findings show that the Privacy Covenant has functioned as a driving force for strengthening data protection. The public education sector organizes themselves, and extensively cooperates with both state institutions and platform companies in order to improve data protection. Many of these stakeholders take more responsibility in protecting the privacy of children and keep on collaborating for the ongoing improvement of data protection. In this collaboration, schools should take into account an observed diversity in platforms which influences the distribution of responsibilities between them.

Keywords: Cooperative responsibility, data protection, platformization; public education

1 Introduction

1.1 Platformization of public education

Platformization is defined as "the penetration of infrastructures, economic processes, and governmental frameworks of digital platforms, in different economic sectors and spheres of life (Poell, Nieborg, and Dijck, 2019, p 5-6)". It is a process that we have seen earlier in sectors like taxi services (e.g. Uber), hotel accommodation (e.g. Airbnb) (van Dijck and Poell, 2015) and the media landscape (e.g. Netflix) (van Dijck and Poell, 2013). In public education, platformization emerges through 'educational technology' (EdTech) platforms that offer technologies that combine IT and educational practices

and facilitate learning. A global industry of EdTech platforms and services is growing and increasingly encompassing every aspect of education including enrolment; online program management; learning analytics; digital libraries; alumni relation management; exam proctoring; plagiarism detection and so on (HolonIQ, 2020; Wiley 2018 in Williamson, 2020). An example of how platformization works is the integration between public education and digital infrastructures of companies like Alphabet/Google and Microsoft. Kerssens and Dijck (2021) show how this works through corporate strategies of intra-operability and public sector strategies of interoperability. Interoperability is a strategy aimed at promoting transparency and openness between a variety of educational technology systems and data flows under public oversight and control. Intra-operability is a strategy that aims at the connection of educational technologies to their central platforms under private control, fostering lock-in effects.

1.2 Impact of platformization on public education

Platformization increasingly changes educational pedagogies, policies, governance, financing and the role of teachers in public education (Cf. Williamson, 2017). It challenges the interests and values of public education, and impacts the governance and control of schools over the pedagogy and organization of public education (Kerssens and Dijck, 2021). The impact on governance indirectly affects the right to privacy and to data protection of children (who are a special category of data subjects in the GDPR that needs strict protection[1]), for example by raising questions about controllership and challenging the implementation of data protection in schools regarding purpose limitation, transparency, as well as extra EU data transfers (Angiolini et al., 2020). Whether schools operate ethically and protect their children's data according to data protection law is questionable (Botta, 2020; Ducato and et al, 2020).

The impact on governance and data protection manifests itself in, amongst others, the construction of data processing agreements (DPA) in which the relationship between schools as data controllers and data processors like Alphabet/Google, Microsoft, Magister or Squla is formally settled according to Art. 28 (3) (EU, 2016). This can be exemplified through the obligation for schools to only contract data processors who provide sufficient guarantees to implement appropriate technical and organizational measures for protecting personal data (EU, 2016, art. 28 (1)), and the obligation to impose detailed instructions on the processing and protection of personal data by data processors, as expressed in Article 28 (3) of the General Data Protection Regulation (GDPR) (EU, 2016). But are schools able to comply to these obligations? Initial drafts of data processing agreements often lay the foundation for negotiating and stipulating guarantees and instructions. However, who drafts the contract may depend on varying power (im)balances which includes market position, technical expertise, and access to legal services. Platforms tend to set up standard terms and conditions that include data processing agreements, often from a 'take it or leave it' perspective, leaving schools uncertain about GDPR compliance. This imbalance in power, however, doesn't absolve schools from their responsibility as data controllers (Olbrechts, 2020).

[1] See for example Art. 6 (1f), Art. 8, and Art. 12 (1) of the GDPR (EU, 2016)

1.3 Remedying the power imbalance

The platformization of public sectors increasingly comes with debate around public values, platform governance, and questions about how to remedy the power imbalance between schools and platforms. Some proposals from academia are to critically assess the integration of technologies in education through strategies of intra-operability, the promotion and securing of interoperability, and an inclusive approach to governance: on, and between, national and supranational levels (Kerssens and Dijck, 2021). Also the promotion of the embedding of data protection principles in the design and development of technologies, more scrutiny by data protection authorities, critical procurement, collective negotiations with platforms and the development of 'public infrastructures' that serve the common good are proposed (Angiolini et al., 2020). GAIA-X is an example in which partners from business, science and politics work since 2019 towards a European Cloud Infrastructure based on European values (Energy, 2020; Funk, 2021). On the national level, the Dutch government's Digital Strategy (Ministerie van Algemene Zaken, 2021) pays attention to public values. Another Dutch example is 'Public Spaces'[2]: an initiative in which a coalition of public organizations in public media, cultural heritage, festivals, museums and education works together 'to reclaim the internet as a force for the common good' and advocates 'a new internet that strengthens the public domain', including for education (Public Spaces, 2021). A similar, European, initiative is recently launched under the name 'Shared Digital European Public Sphere' (SDEPS)[3].

The Dutch public education sector is also actively working to secure public values like equality, privacy, and accessibility. It has initiated several collective initiatives, like a number of Data Protection Impact Assessments (DPIA) into Google Workspace for Education[4] and the biggest Learning Management System (LMS) providers (ESIS, ParnasSys, Magister, Somtoday and SchoolOAS)[5], who serve a huge majority of schools with their products and services (Kerssens & Dijck, 2021), and constructed a 'value framework'[6] for the use of ICTs. The sector has also constructed the (legally obliged) 'ECK-iD' [7], a technical standard and a privacy-friendly way to exchange personal data between different systems that allows schools to control data flows (ECK-iD, 2021). Such a standard helps "the sector to jointly exercise public control over digitization by designing interoperability as a collective principle (Kerssens & Dijck, 2021 P. 10)". The sector now also calls for a European interoperable system in which public education can profit from technology innovation, but keeps the data in public hands (SURF, 2021).

---

2 https://publicspaces.net/

3 https://sdeps.eu/

4 https://www.privacycompany.eu/blogpost-en/privacy-assessment-google-workspace-g-suite-enterprise-dutch-government-consults-dutch-data-protection-authority-on-high-privacy-risks

5 https://www.kennisnet.nl/artikel/12377/dpias-op-leerlingadministratiesystemen/

6 https://www.kennisnet.nl/artikel/12352/waardenwijzer-in-gesprek-over-onderwijswaarden-en-digitalisering/

7 https://www.eck-id.nl

1.4 Cooperative responsibility

We propose 'cooperative responsibility' as a participatory approach to remedy the power imbalance between schools and platforms. Inspired by the work of technology philosopher Andrew Feenberg and social constructivist perspectives of Science & Technology Studies (Cf. Pinch & Bijker, 1984), we believe that powerful (Big Tech) platforms and subordinate groups like schools (which we call stakeholders) 'fight' over the future of public education. Feenberg's Critical Theory of Technology (Feenberg, 1999) argues that technologies are not neutral but have values and interests of people inscribed through its design and development. These 'formally biased' technologies usually embody and reproduce the values and interests of dominant forces, like those of EdTech platforms. However, sometimes also subordinate groups involved in the design and development can influence the construction of technologies. Feenberg calls this 'democratic rationalization'. Thus, schools are able to influence the design and development of platforms in education and preserve public values like protection the privacy of school children.

Platforms have become so important in public sectors that they have started to play a vital role in the realization of public values. But how, and to what extent, do platforms take up responsibility for this? Platforms operate relatively independent of public governance and distance themselves often from their responsibility. Discussions around platform governance, then, often depart from the standpoint that platforms have to be held accountable, focusing to a large extent on the responsibility of one actor (e.g., data controller, data processor, editor, host, gatekeeper). But platforms are by their very architectures only partly able to exercise such control (Helberger et al., 2018 p. 2). Users are responsible as well.

Scholars have approached the power of online platforms from different perspectives (De Gregorio, 2021 p. 42). One of these perspectives is 'cooperative responsibility' (Helberger et al., 2018). This theory argues, contrary to the 'one actor' approach, that unilateral governance of platforms for the realization of public values doesn't work. Instead, it should be the result of a dynamic interaction and allocation of responsibilities between platforms and users, supported by a legal and policy framework created by state institutions (government). These responsibilities should be both backward-looking (retrospective, such as who is responsible for occurred data breaches or bad security) and forward-looking (prevention, like creating awareness and data literacy, privacy by design and critically assessing cookie notices by users). How these responsibilities are distributed depends on specific contexts of power, expertise, capacities, resources, values, and interests of stakeholders. Here, cooperative responsibility follows Fahlquist's argument (2009 p. 115-116) that "power and capacity entails responsibility": users don't have the same power as companies and the government, and users are not always able to take responsibility, unless they collaborate (which is not always the case). For this reason platforms and government have strong forward-looking responsibilities to empower users so they can take their responsibilities (Pierson, 2012). For example, platforms should encourage users to meaningfully assess the consequences of cookie consent, and restrain from designing dark patterns, while the government should stimulate and facilitate cooperation between stakeholders.

To operationalize cooperative responsibility, Helberger et al (2018) developed a framework including four key steps: 1) the context-specific, collective identification of public values; 2) the distribution and acceptance of responsibility between actors in a value network; 3) a multi-stakeholder process of public deliberation to advance the identified public values; and 3) the translation of public deliberation into regulations, codes of conduct, terms of use, and the design of technologies. Our research question is therefore: How is cooperative responsibility operationalized in an 'on the ground' setting in public education, where data controllers and data processors actually have to enter into data processing agreements with each other?

1.5 The case of the Privacy Covenant

As discussed, drafts of data processing agreements can be drawn up by the data controller or the data processor. 'Models' of data processing agreements are often provided to groups of data controllers and data processors by organizations that represent their (public) sectors and stakeholders. These models can be used by data controllers as a draft for negotiating and stipulating detailed instructions with data processors. When we look at the construction of these models in the public sector in the Netherlands, we see different forms, covering at least the main requirements as expressed in Article 28 of the GDPR. Some can be used and be adjusted freely, others are stricter. Some standards are mandatory for data controllers like the one of the Dutch Association of Municipalities (VNG, 2021), some are voluntary such as the standard made for Housing Associations in the Netherlands (Aedes, 2018). The standard data processing agreement of the Dutch Healthcare organizations (Brancheorganisaties Zorg, 2017) is required by some data controllers in the sector. In public education in the Netherlands, SURF, a cooperative association of Dutch educational and research institutions provides the 'SURF Framework of Legal Standards for Cloud Services' including a "Model Processing Agreements" and accompanying documents like a Safety Measures Guide (SURF, 2019). Sector organizations that represent schools in primary (PO-Raad) and secondary education (VO-raad), as well as vocational secondary education (MBO-Raad), and three trade organizations that represent publishers that develop and supply learning material, tests and educational services to public education ('GEU')[8], distributors of textbooks for public education ('KBb-Educatief')[9] and digital education suppliers (VDOD)[10] also drafted a model data processing agreement. This model is part of the broader 'Convenant Digitale Onderwijsmiddelen en Privacy', or in short 'Privacy Covenant'[11] (PO-Raad et al, 2018). A covenant is a form of an umbrella agreement in which all stakeholders agree upon the protection of personal data of school children in general. To answer the research question, we have conducted a case study into the construction, meaning and relevance of the Privacy Covenant. The objective of our research is to empower data controllers in data protection by giving insights into how this

[8] https://geu.nl/english/
[9] https://www.boekbond.nl/kbb-educatief/
[10] https://vdod.nl/
[11] https://www.privacyconvenant.nl/

can be done through an example of cooperative responsibility. Where we speak of the Privacy Covenant, this includes the accompanying model data processing agreement.

2 Methodology

This research reports on a qualitative case-study (Yin, 2014) conducted in public education in the Netherlands in which we analyze the construction of the 'Privacy Covenant' through the lens of the framework for cooperative responsibility. We analyzed both the process of constructing the Privacy Covenant, as well as its issues, pros and cons while used in practice. We conducted 6 semi-structured interviews with stakeholders (representatives from schools, from a privacy consultancy, from SURF and SIVON - a cooperative procurement organization for education -, and from one of the trade organizations) that have participated in the construction of the Privacy Covenant, and 8 semi-structured interviews with school employees (university of applied sciences, secondary- and secondary vocational education) for whom drawing-up and checking data processing agreements before they are signed by the schoolboard is part of their job. We choose this 'on the ground' setting to investigate how stakeholders actually manage agreements between them and what motivates them (Bamberger & Mulligan, 2018). We selected the interviewees based on purposeful sampling, and on the following background criteria: business, legal and ICT, to guarantee a variety of insights from different perspectives (Table 1).

Table 1. Selection of interviewees and backgrounds

#	**Interviewee from**	**Background**
i1	Universities	ICT
i2	Universities	Legal
i3	SURF	Business/ICT
i4	Universities	ICT
i5	Secondary education	ICT
i6	Secondary education	ICT
i7	Secondary education	Business
i8	Secondary vocational education	ICT
i9	Secondary vocational education	Legal
i10	Secondary education	Business
i11	EDU-K	Legal
i12	SIVON	Legal
i13	Privacy consultancy	Business
i14	Trade organization	Legal

Interviews were transcribed with a combination of the transcription functionality in MS Word as well as through the qualitative research software MAXQDA, which has also been used to analyze the results.

3 Results

3.1 Defining public values for public education

The construction of the 'Privacy Covenant' started in 2013 when the Dutch Government initiated the 'Breakthru projects ICT', aimed at stimulating ICT innovation and its potential for economic growth, as well as tackling societal challenges. One of the projects was the 'Breakthru project Education & ICT', a partnership between the Dutch government and the public education sector. The main (societal) goal of the project was stimulating personalized learning so that justice is done to the diversity in learning capacity and needs of children, and to optimally support them in developing their talent. This goal, then, supports the Dutch position in a globalizing economy and economic growth. The importance of privacy as a public value has been acknowledged as a precondition for realizing the potential of personalized learning already from the start of the project, when, initiated by the government, stakeholders from both schools as well as companies started talks about data protection.

3.2 Allocating responsibility in data protection

The different stakeholders (companies, users, and state institutions) have taken a diversity of responsibilities.

Companies
We focus on national and international EdTech companies whose products and services are being used in Dutch public education. Our research shows that there are huge differences between companies that affect the power imbalance between schools and companies. Indicators that we used to categorize companies are: the ability of schools to impose detailed instructions and to get sufficient guarantees by the data processor; who drafts the data processing agreements; represented by trade organization or not; and usage of the model data processing agreement (Table 2). The categories are: 1) the 'Chain Partners': a diverse, often powerful group of Dutch companies like Topicus, Iddink, ThiemeMeulenhoff and VanDijk that are to a great extent represented by the three private trade organizations GEU, KBb-Educatief and VDOD and/or have huge market shares with their software products; 2) Big Tech (which often refers to US companies Alphabet/Google, Microsoft, Apple, Meta Platforms/Facebook and Amazon, and in public education in the Netherlands predominantly to Alphabet/Google and Microsoft): a very powerful group of companies that due to their technical expertise, financial means and infrastructural power plays a very dominant role in public education in the Netherlands; 3) all other, (assumed) less powerful, companies (mostly referred to as 'small' companies or examples of start-ups); and 4) 'independent apps' (those

companies that have entered into contract with children/ students themselves like TikTok and Duolingo). See Table 2 for an overview and summary of the categories and the power distribution between different groups of companies and schools, where it should be emphasized that each company is unique, and that this categorization has only been made for the clarity of our analysis.

In the first category (Chain Partners), a group of publishers (e.g. Noordhoff and ThiemeMeulenhoff) and distributors (e.g. VanDijk and Iddink) has a long powerful history in public education as book suppliers that have expanded their portfolio with digital learning material. Digital education suppliers such as Heuitink.ict and CITO are also part of the group of Chain Partners. The trade organizations GEU, KBb-Educatief and VDOD, of which the Chain Partners are members, are at the center of how digital education is being shaped: they participated in the construction of the Privacy Covenant and are also members of EDU-K, a platform in which the private trade organizations and public sector organizations talk about, and work together for a better functioning, educative ICT chain, and create the conditions for the successful application of ICT in learning through e.g. privacy, security, standardization and accessibility of digital learning material (EDU-K, 2021). When looking at the allocation of responsibilities between the Chain Partners and schools, the main issue in the early discussions of the Privacy Covenant was the interpretation of 'data controllership'. The publishers, that amongst others also process personal data and provide learning analytics based on this data, maintained the view that they were data controller, a position that would enable them to commercially exploit personal data. On the contrary, the standpoint of the schools was that not the publishers, but they themselves were data controllers and that the publishers were data processors and thus processed the data under responsibility of the schools. This dispute was only settled after a lot of media attention and critique around the processing of personal data of minors by publishers[12] as well as the involvement of the Dutch Data Protection Authority through the 'Snappet'-case[13]. From that moment, schools are in principle appointed as data controllers and all companies that process data on behalf of schools as data processors. Only if companies have a direct relationship with children or their parents, and not via the school, they are the data controller themselves. This is for example the case of many apps like TikTok, YouTube or Duolingo that are being used by teachers and students, often out of sight of the schools (category 4 in Table 2). The settlement of this discussion might look like just a legal interpretation of the GDPR, but it was, in line with the second step of cooperative responsibility (the distribution and acceptance of responsibility between actors in a value network), an important milestone for 'data protection-maturing' schools in the discussions around the growing and unregulated use of personal data by a plethora of companies in Dutch public education. Apart from the discussion about data controllership, the Chain Partners take responsibility by helping schools to fulfill their GDPR requirements by providing assistance in filling in the data processing agreement. This form of forward-looking responsibility is very useful as these companies have more expertise and are more familiar with the data processing and the organizational and technical

[12] https://www.rtlnieuws.nl/nieuws/bundel/1497271/privacyschending-basisscholen

[13] https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-constateert-overtreding-wet-bij-snappet

measures they apply. It also stimulates the actual and correct use of the model. This correct use is, however, still not a given: the model data processing agreement is not always used and if it is, it is sometimes changed unilaterally (e.g. liability) by companies. Besides taking these responsibilities, the DPIA into some of the Chain Partners has shown that they should take even more forward-looking responsibility by: empowering schools regarding access control; privacy by design/default (e.g. deleting certain fields); security measures (e.g. multifactor authentication); handling data retention periods; and data transfers to third parties.

The second to the fourth category of companies are not represented by one of the private trade organizations[14]. Companies in the second category, 'Big Tech' companies like Google and Microsoft, are also not a participant in the Privacy Covenant. Big Tech mostly dictates the rules of the game as expressed in their own data processing agreements where they take a 'take it or leave it' approach. Schools (must) have a lot of confidence in the expertise of Big Tech and rely to a great extent on the (discourse related to) data protection efforts made by these companies. However, Big Tech companies pose many risks for data protection as is again and extensively shown through the aforementioned DPIA's conducted on Google Workspace for Education and on Microsoft Office tools. In the 'power struggle' between schools and Big Tech, both SURF and SIVON are well equipped to help, as they have shown in the agreement with Alphabet/Google on the mitigation of 11 high risks for data protection in Google Workspace for Education[15]. Or as one interviewee said: "the discussion should not be only about Big Tech, but with Big Tech" (i3, SURF, business/ICT), which can result in improvements in data protection.

The third category of companies consist of all other, (assumed) less powerful, platform companies. Examples are start-ups, 'small' companies, and photographers. Schools are worried about their ability to sufficiently protect personal data and say that questions about data controllership are possible again.

The fourth and last category consists of 'independent apps'. These companies have not entered into contract with the school, but with minors, their parents or teachers themselves. Examples of independent apps are TikTok, Kahoot, Duolingo and YouTube. The apps are frequently used by teachers and minors for learning purposes: "(…) and then they [children during classes] are going to dance and shoot short videos etc.…" (i5, secondary education/ ICT). However, the use of these apps could clash with the responsibility of schools for data protection. Of course, as data controllers, the companies behind the apps have their own responsibilities towards data protection, but they are no stakeholder in the Privacy Covenant and have not entered into a data processing agreement with the school at all. Independent apps come and go and as such continuously reconfigure and complicate discussions around data protection by these apps.

---

[14] However, Microsoft is member of trade organization VDOD and participated in some of the earliest meetings of the construction of the Privacy Covenant.

[15] https://www.sivon.nl/actueel/akkoord-onderwijs-met-google-over-privacyrisicos/

Table 2. Distribution of power between different groups of platform companies and the school

	Category	Detailed instructions/ guarantees	Usage model DPA
Data processors represented by trade organizations	1 - Chain partners (powerful) like Topicus, Iddink, VanDijk and ThiemeMeulenhoff	Detailed instructions dependent on data processor; sufficiency of guarantees given by companies are unchecked by schools	Chain Partners participate in the privacy covenant, have to use of the model, but do often derogate from it; data processing agreement provided by the company; data processing agreement is not periodically checked and updated
Data processors (mostly) not represented by trade organizations	2 - Big Tech (powerful) in Dutch education predominantly Alphabet/Google and Microsoft	Detailed instructions dependent on data processor; schools have confidence in sufficiency of guarantees given by companies	No subscriber privacy covenant; data processing agreement provided and updated by the company (take it or leave it approach); data processing agreement is not periodically checked and updated
	3 - All other platform companies (less powerful data processors) like (some) start-ups and 'small' companies	Detailed instructions dependent on data controller or data processor; schools have worries about the sufficiency of guarantees given by companies	Companies can be a participant in, or a supporter of the privacy covenant; they mainly use the model as provided schools; schools more critical towards small parties; data processing agreement is not periodically checked and updated
	4 - Independent apps (can be powerful) like TikTok and Duolingo	N.A.	N.A.

Users

The second group of stakeholders are the users (schools, minors/parents, and representatives of these groups). In cooperative responsibility, it is this group that has to be empowered by companies and the government (as respectively has been and will be discussed in the former and next paragraph).

In schools, we discern people working at schools (e.g. schoolboard, teachers and other employees). There are differences between schools in their ability to take responsibility in data protection, mainly because of differences in size, expertise, and financial means available. Not all schools (are able to) take their responsibility as a data controller. Data processing agreements provided by platform companies are for example

sometimes approved and signed by schools based on gut feelings. Or as one interviewee said: "it's just signing or also looking at the content [..] it depends on the school or who the schoolboard is (i14, trade organization, legal)". It looks like that the bigger the school, the more 'professional' the school can operate, and the more resources and expertise are available for data protection. In this regard, MBO-schools are better positioned to tackle these problems and take the responsibility needed, as these schools are much more consolidated and have more means for data protection: "they [MBO-schools] are really professional organizations, they do really look at the data processing agreement (i14, trade organization, legal)". Further research must show to what extent this claim can be substantiated. Interesting is how the education sector is empowering itself via numerous ad hoc and (more) formal collaborations through which schools are being represented in data protection. Examples of these collaborations are: Kennisnet (the ICT support organization for primary, secondary and vocational secondary education which is subsidized by the government); SURF, SIVON , EDU-K, and SAMBO-ICT (an IT network in MBO), which are all cooperatively organized; the 'Information Security and Privacy Networks' in which data protection and security experts from schools participate, facilitated by Kennisnet; 'SCIPR' (a community for privacy and security in higher education that is facilitated by SURF); and the sector organizations PO-Raad, VO-raad, and MBO-Raad that represent schools in the construction of the Privacy Covenant.

The second group of users are minors/parents. This group depends to a great extent on the data protection efforts made by schools and the aforementioned collaborations. 'Ouders & Onderwijs' is an organization for parents that was consulted during the early discussions around the Privacy Covenant but did not participate because they trusted the parties in constructing an adequate covenant. In the group of parents, we see an emerging tendency of democratic rationalization (Feenberg, 1999), with parents that increasingly criticize data protection of schools and in that way contribute to its improvement: "We more and more get critical questions of parents because they are increasingly aware of GDPR, with which they have to deal with in their work as well. Schools that don't mature in this and don't involve parents, will face critical parents (i12, SIVON, legal)".

Government

The government, the third and last group of stakeholders involved, includes the Ministries of Education, Culture and Science (OCW)[16] and Economic Affairs (EZ)[17], Kennisnet[18] and the Dutch Data Protection Authority[19]. The government takes its responsibility by for example implementing data protection law. It also supports schools directly through facilitating and stimulating the Privacy Covenant and data protection in general via Kennisnet that is publicly funded by the government. The government also cooperates with the education sector in conducting DPIAs like the one on Microsoft products,

[16] https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap
[17] https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat
[18] https://www.kennisnet.nl/
[19] https://www.autoriteitpersoonsgegevens.nl/

and through the publicly funded Rathenau Institute[20] which cooperates for example with the education sector in the construction of the 'value framework'.

3.3 Public deliberation and the translation of data protection into an agreement: the Privacy Covenant in practice

The construction of a 'Privacy Covenant' started in 2013 and the first version was finally agreed upon in 2015. The Covenant, now in its' version 3.0, is formally positioned under the responsibility of EDU-K. The "Ketenadviesgroep Privacy", part of EDU-K, maintains and develops the Privacy Covenant, and also handles complaints from stakeholders. All schools and all companies that are represented by one of the sector/trade organizations have to become a participant of the Privacy Covenant. But where schools are most of the time automatically participant of the Privacy Covenant, different rules apply for companies that process data on behalf of schools. Companies can only sign up to the Privacy Covenant if they have a contract with one or more school(s), process personal data, and provide (digital) education systems and services. The latter provision is a source for much debate around the definition of '(digital) education systems and services' and the wish of many companies that process data, from photographers to printers, to participate in the Privacy Covenant. These companies en masse subscribed themselves because they saw it as a certificate of 'good practices in data processing'. However, the Privacy Covenant is tailored to suppliers of digital learning materials and as such the Privacy Covenant and its model data processing agreement have no added value for other companies. The solution is now that these companies can become a 'supporter' and can make use of another model data processing agreement. If the requirements for becoming a participant are met, companies can become participant of the Privacy Covenant by signing a letter of intent and thereby commit themselves to its rules. It should be emphasized that signing up to the Privacy Covenant as well as the use of the model is not mandatory *by law*, and schools can always decide to do otherwise. Even if stakeholders are signed up to the Privacy Covenant, they are not legally bound to obey its rules and use the model. However, signing up to the Privacy Covenant implies the mandatory and correct use of the model data processing agreement. In practice, this is not a given as for example sometimes the model is used, but adapted by one of the parties, and sometimes a data processing agreement is signed 'right by the X', without being reviewed, or eventually not signed at all. In other cases, different models are being used. To tackle this, trade organizations now check their members for the correct use of the model by assessing participants and to let them sign a declaration. Clearly, the process of actually drawing up data processing agreements in public education is far from straightforward and the stakeholders are still in the process of improving this process.

[20] https://www.rathenau.nl/en

4 Discussion

The Privacy Covenant is an example of how the public education sector, (platform) companies and state institutions cooperatively shape data protection. Privacy is an important value in education, not least because it concerns the privacy of children and is a special category of data subjects in the GDPR, and the massive collection of personal data needed for personalized learning can seriously harm the future of young people as a child's data profile can be used for many purposes such as credit checks, assessments of insurance rates, and hiring processes. We have seen strong commitment to data protection of all stakeholders.

We found a distinction of categories of companies which influences the way responsibilities between schools and platforms are being distributed. The first category of companies, represented by trade organizations, is intensively involved in the construction of the Privacy Covenant and beyond (like in the example of EDU-K). This is not only beneficial regarding for example providing (legal) clarity and efficiency to their members, it also benefits their commercial and political interests as participating in the construction of the Privacy Covenant enables them to influence the rules of the game. According to Fahlquist (2009) this power comes with responsibilities, something which the representing trade organizations take in various forms. However, the Chain Partners only represent about 20% of the participants and supporters of the Privacy Covenant. For example, an important and dominant company in education in the Netherlands like Alphabet/Google, start-ups as well as children and parents have not actively been involved in the construction of the Privacy Covenant. From a cooperative responsibility perspective these stakeholders should also be involved. The second category of companies (Big Tech) in general has a great responsibility due to their omnipresence and power in education. They have the responsibility to be transparent and make their systems privacy by design. However they also have responsibilities towards many other platform companies that supply software to the education sector, as Big Tech companies are often the providers of the infrastructures (e.g. cloud-, analytics- and security facilities) on which many of these companies build their software (Poell, 2018). Schools should take more forward-looking responsibility towards the third ('small' companies) and the fourth category (the broadly used 'independent apps' like TikTok and Duolingo that have no contract with the school) of companies, for example by determining data controllership in the relation with new companies, and by initiating, drawing up and following up data processing agreements. Schools can also restrict the use of apps that have not entered into contract with them, and/or conduct DPIA's on them.

Schools often lack the expertise and means to take full responsibility for data protection. Schools could empower themselves by cooperating with other schools regarding data protection (e.g. joint DPO, privacy officer, joint policy etc.), by facilitating more financial means, awareness and data literacy (e.g. of teachers) in schools, by cooperating with SURF and SIVON in taking more responsibility towards companies like TikTok and other Big Tech companies, and by seeking the view of children and parents. Regarding the latter, Article 35 of GDPR even "explicitly demands to 'where appropriate, […] seek the views of data subjects or their representatives on the intended processing' in so-called Data Protection Impact Assessments (DPIA) (Breuer & Pierson,

2020)". Finally, schools that lack expertise and means could also be empowered by the government, e.g. through the support of Kennisnet.

In our analysis we focused on three main types of stakeholders: platform companies, users, and state institutions. In further research we aim to broaden and refine the value network with additional stakeholders, as proposed by Helberger et al (2018, p. 12). The four categories of companies we identified (see Table 2) can thereby be the focus to further enrich our understanding. Next, we also found that deploying the high level four steps of the cooperative responsibility for our analysis was not always straightforward. Our future research aims at further operationalizing this framework, foremost based on comparative analyses of different case studies.

5 Conclusion

Processes of platformization increasingly impact the governance of public education. This manifests itself in the construction of data processing agreements in which the relationship between schools and (platform) companies that process data on behalf of schools, is formally settled according to Art. 28 (EU, 2016). Through a qualitative analysis of the construction of the Privacy Covenant, an umbrella agreement in which both schools and companies agree upon the protection of personal data of school children in general, we investigated 'cooperative responsibility' as a participatory approach to platform governance in schools. The results show that the Privacy Covenant has functioned as a driving force for strengthening data protection and as a remedy for power imbalances between platforms and schools. Collaborations like the Privacy Covenant can be successful as now all stakeholders take more responsibility in protecting the privacy of children. The results also show that the public education sector organizes themselves very well for data protection, and in this regard extensively cooperates with both platform companies and state institutions on the ongoing improvement of data protection. In the collaboration with platform companies, schools should take into account an observed diversity in platforms (Chain Partners, Big Tech, all other platforms, and independent apps).

6 References

Aedes. (2018). *Gegevensbescherming verwerkt in nieuw Model Inkoopvoorwaarden*. Aedes. https://www.aedes.nl/artikelen/bedrijfsvoering/inkoopsamenwerking/gegevensbescherming-verwerkt-in-nieuw-model-inkoopvoorwaarden.html

Angiolini, C., Ducato, R., Giannopoulou, A., & Schneider, G. (2020). *Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education* (SSRN Scholarly Paper ID 3779238). Social Science Research Network. https://papers.ssrn.com/abstract=3779238

Bamberger, K. A., & Mulligan, D. K. (2018). Privacy Law – on the Books and on the Ground. In B. van der Sloot & A. de Groot (Eds.), *The Handbook of Privacy Studies* (pp. 349–354). Amsterdam University Press; JSTOR. https://doi.org/10.2307/j.ctvcmxpmp.19

Botta, J. (2020). *The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A*

Data Protection Challenge for Universities. Brussels Privacy Hub.

Brancheorganisaties Zorg. (2017). Modelverwerkersovereenkomst voor de zorgsector. *Brancheorganisaties Zorg*. https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

Breuer, J., & Pierson, J. (2020). The Right to the City and Data Protection for Developing Citizen centric Digital Cities. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2020i0.11178

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001

Ducato, R., & et al. (2020, June 4). *Emergency Remote Teaching: A study of copyright and data protection policies of popular online services (Part II)*. Kluwer Copyright Blog. http://copyrightblog.kluweriplaw.com/2020/06/04/emergency-remote-teaching-a-study-of-copyright-and-data-protection-policies-of-popular-online-services-part-ii/

ECK-iD. (2021). *Veilig digitaal leren: ECK iD*. ECK. https://www.eck-id.nl

EDU-K. (2021). *Edu-K*. Edu-K. https://www.edu-k.nl

Energy, F. M. for E. A. and. (2020). *GAIA-X - the European project kicks off the next phase*. https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.html

EU. (2016). *Regulation (EU) 2016/679 of the european parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fahlquist, J. N. (2009). Moral Responsibility for Environmental Problems—Individual or Institutional? *Journal of Agricultural and Environmental Ethics*, *22*(2), 109–124. https://doi.org/10.1007/s10806-008-9134-5

Feenberg, A. (1999). *Questioning Technology*. Routledge.

Funk, M. (2021). *The European Strategy on Data—Analysing GAIA-X's influence strategy in light of the EU Commission's digital strategy from a Multi-level Governance perspective*. http://lup.lub.lu.se/student-papers/record/9045107

Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, *34*(1), 1–14. https://doi.org/10.1080/01972243.2017.1391913

HolonIQ. (2020). *2021 Global Learning Landscape.* https://globallearninglandscape.org/index.html

Kerssens, N., & Dijck, J. van. (2021). The platformization of primary education in The Netherlands. *Learning, Media and Technology*, *0*(0), 1–14. https://doi.org/10.1080/17439884.2021.1876725

Ministerie van Algemene Zaken. (2021, April 26). *Nederlandse Digitaliseringsstrategie 2021—Kamerstuk—Rijksoverheid.nl* [Kamerstuk]. Ministerie van Algemene Zaken. https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/nederlandse-digitaliseringsstrategie-2021

Olbrechts, A. (2020, September 7). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* [Text]. European Data Protection Board - European Data Protection Board. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

Pierson, J. (2012). *Online Privacy in Social Media: A Conceptual Exploration of*

Empowerment and Vulnerability (SSRN Scholarly Paper ID 2374376). Social Science Research Network. https://papers.ssrn.com/abstract=2374376

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

PO Raad et al. (2018). *Verwerkersovereenkomsten*. Aanpak informatiebeveiliging en privacy in het onderwijs. https://aanpakibp.kennisnet.nl/verwerkersovereenkomsten/

Poell, T. (2018, December 4). *Boekpresentatie: The Platform Society*. https://www.youtube.com/watch?v=w13dL2QNbzg

Poell, T., Nieborg, D., & Dijck, J. van. (2019). Platformisation. *Internet Policy Review*, *8*(4). https://policyreview.info/concepts/platformisation

Public Spaces. (2021). *What is Public Spaces?* PublicSpaces. https://publicspaces.net/english-section/

SURF. (2019). *SURF Framework of Legal Standards for (Cloud) Services | SURF.nl*. https://www.surf.nl/en/surf-framework-of-legal-standards-for-cloud-services

SURF. (2021). *Terugblik seminarreeks publieke waarden—Deel II | SURF.nl*. https://www.surf.nl/surf-magazine/surf-magazine-in-gesprek-met-bestuurders-over-publieke-waarden/terugblik-0

van Dijck, J., & Poell, T. (2013). *Understanding Social Media Logic* (SSRN Scholarly Paper ID 2309065). Social Science Research Network. https://papers.ssrn.com/abstract=2309065

van Dijck, J., & Poell, T. (2015). *Higher Education in a Networked World: European Responses to U.S. MOOCs* (SSRN Scholarly Paper ID 2645629). Social Science Research Network. https://papers.ssrn.com/abstract=2645629

VNG. (2021). *Handreiking Standaard Verwerkersovereenkomst Gemeenten (VWO)*. Informatiebeveiligingsdienst. https://beheer.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/

Williamson, B. (2017). *Big Data in Education: The Digital Future of Learning, Policy and Practice*. SAGE.

Williamson, B. (2020). Making markets through digital platforms: Pearson, edu-business, and the (e)valuation of higher education. *Critical Studies in Education*, *0*(0), 1–17. https://doi.org/10.1080/17508487.2020.1737556

Yin, R. K. (2014). *Case study research: Design and methods*.