Teil V – Praktische Umsetzung(en) – Erfahrungsberichte und Handlungsempfehlungen

A day-in-the-life of a datafied child – observations and theses

Jen Persson

Abstract

"*Children do not lose their human rights by virtue of passing through the school gates.*" The UN Committee on the Rights of the Child set out a clear message in 2001. As the use of electronic school records has expanded rapidly in the twenty years since, however, children's rights have not only been left at the school gates but have become lost in the digital environment in which companies follow online activity from school into the home, 24/7, and every day of the year. I describe some of the practices in the state education system in England, where children attend compulsory education from their fifth birthday, and immediately lose control of their digital footprint. At the time of writing, there has been little enforcement of GDPR in education, and there is a lack of attention paid to laws in edTech thinking. I propose actions needed to build a rights' respecting environment in education, and areas for further research in emerging harms, with the aim of preventing known interferences with rights today; reducing personal, institutional and state security risks; and horizon scanning, to protect the future of children's autonomy, human rights, state education, and society.

1. Children do not lose their human rights by virtue of passing through the school gates, but they are not well realised:

1.1 In 2017 the Children's Commissioner in England concluded in a report called 'Growing Up Digital', 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 digital footprint is difficult for adults, it is even harder for children in compulsory education where they are disempowered by default.

1.2 In addition to personal data collected directly from families for the administration of a child's education and care; invisible or inferred information are collected about pupils; through RFID (Taylor 2019), beacons,

virtual assistants in the classroom and by Internet Connected Things. A child's permanent digital record may include standardised test scores but also opinion and inferences, such as behavioural records recorded by a teacher in a school core information management system, an app, or created by artificial intelligence (AI).

1.3 Children care about their privacy and want to be able to decide what information is shared with whom. That is difficult when *"teachers are unclear what happens to children's data and there is common misunderstanding of how much data leaves a school."* (Stoilova et al. 2019).

1.4 If children do not know where their digital footprint goes, they cannot understand how others may use it to make decisions about them. This is amplified when school records are linked with other personal data about them held by the state, by companies, or linked to data purchased from third-party data brokers (WhatDoTheyKnow 2018).

1.5 Rights may not be realised if there is no way to understand them or the choices that the individual has as a result, or there is no clear route for redress when they are infringed upon. Emerging harms and infringements to children's privacy rights under the *General Data Protection Regulation (GDPR)* and Convention 108[1], to their dignity, free expression (Kaye 2019), and their rights enshrined in the UN Convention on the Rights of the Child (UNCRC) to full development and human flourishing, can result from various areas of commercial and state practice that stem from mining the 'datafied child' (Lupton/Williamson 2017). These may be obvious institutional (BBC 2019), personal privacy, or security breaches, but hidden harms may remain to be exposed, such as discrimination and racism or bias in automated decision-making.

1.6 A child's best interests are not consistently defined or considered as part of one-size-fits-all risk assessments in digital procurement processes today, that may not assess special educational needs, ethnicity, or lack of access to technology at home, as part of equality duties.

1.7 There need be no conflict between privacy and innovation (Denham 2017), yet some products in emerging fields infringe on rights when pupils are compelled to use a product, and their interactions are used as the source of training data. The effects of personalisation or of AI on children's wellbeing are largely opaque to families.

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

1 Convention 108. Online verfügbar unter: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108 [Abfrage am 4.10.2020].

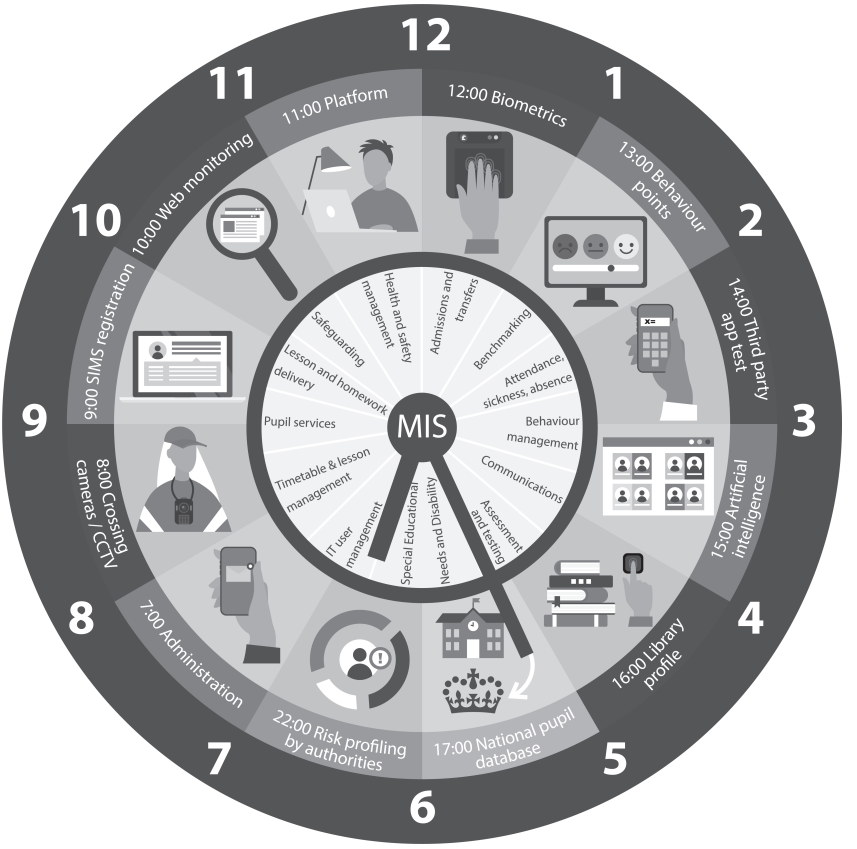
should children be used as continuous research subjects? For a company, a year could be a short time to bring a product onto the market, or to discover the efficacy of an edTech tool is poor, but it could be a defining year of a child's education.

1.9 To be able to give children the tools to be the agents of their own lives, and enable them to realise their rights as fully fledged right holders, we need a sector-wide new approach.

2. What does a day-in-the-life of a datafied child look like?

2.1 To demonstrate the variety of data processing across the range of activities in a child's day, this illustration gives an example of an imagined eleven-year-old's day in a state school. The Data Wheel captures the administrative areas for which a school processes a child's data using a core Management Information System (MIS) at its centre. A variety of private companies offer these to the education sector in England, and also work in collaboration with the national Department for Education to ensure interoperability with the national government data collection every school term, in the school census. In addition, illustrated in the outer ring, children have daily interactions with a wide variety of external third party tools.

Fig 1. An illustrative summary of an eleven-year-old's day in the English school system. Designed by and created from research by the author. Artwork created by Nadia Snopek.



2.2

- 07:30 An event reminder arrives on a child's mobile phone.
- 08:30 She walks to school via the street crossing and is filmed on the patrol officer's bodycam and on closed circuit television (CCTV) at the school entrance, as she enters the playground and the corridors.
- 09:00 Attendance is registered on the school management information system (MIS).
- 09:15 She has logged onto Google classroom, and silently the school web monitoring software starts up, comparing every Internet search

term against a set of thousands of keywords that will trigger a system alert if found. Artificial Intelligence supported software looks for risk indicators of self-harm, mental health, bullying, stranger-danger, terrorism and extremism. Her quick search for information about the cliffs from the family walk she enjoyed that weekend, triggers a flag as potential suicide risk. That notification is sent from the company support staff to a school teacher's inbox.

- 10:00 She is asked by the maths teacher to use an app on her personal mobile phone, to do a quick quiz. She enters her username, school email address and data of birth as verification. The teacher sees all scores and progress on their own screen.
- 11:00 In chemistry she logs into the AI-led platform, and watches a short film. She wasn't paying attention and only gets six out of ten on the multiple choice quiz: Watch it again, suggests the machine learning app, having recorded her mouse movements every two seconds, otherwise she cannot proceed to the next chapter.
- 12:00 Reaching the front of the line to pay for her lunch without cash, she pushes her finger into the unclean machine (Leaton Gray/Phippen 2017) to read her biometrics for the tenth time that week. Every child must use the systems to not only buy lunch, but also to borrow a library book.
- Before they leave that day, the children will have logged into three more apps, including a foreign language app matching vocabulary to pictures, and a reading app to measure the number of words of fiction they read a week. Any child whose profile shows a slowdown in reading speed over a month, will be required to see the librarian.
- At the after-school football club pupil attendance is checked against their names from the school information management system provided details. Their sports changing space is recorded on CCTV. Their team photo was taken for the school website, social media pages, and local newspaper for the tournament that weekend. She feels left out as the only one whose parents have refused photographs for marketing.
- 18:00 At six pm, she logs back into Google classroom, accessing her homework tasks and contents at home. She watches a YouTube video, and all the time the web monitoring is scanning her Internet screen content for signs of suicide. She's on a watch list now since this morning's system error. But she 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, and policing records and build predictive profiles for interventions.

- Once a term, three times a year, her details from the Management Information System are sent in the school census to the National Pupil Database, now holding the named records of over 21 million people in England. (defenddigitalme 2018)
- Years later, her school records will be joined to data from her university application records, and her first employment earnings and / or state welfare payments, will suggest to civil servants how much each education costs the state and be used by politicians to tell the public which courses have the greatest economic return.

2.3 She has no idea to how many companies in which countries her personal data has been sent in the course of this day, or knowledge of the national databases. The implications for the future of society are staggering if we can no longer rely on privacy as an enabling right to participation, to protect full and free development of personhood and character free from excessive or opaque influence of behaviour, to protect the right to access confidential information without surveillance, or to move into adulthood without being held back by predictive profiling used to deny opportunities to pupils less likely to succeed, used in secret to deny eligibility for student loans (Adams 2018) or passed on from school to Higher Education.

3. The sensitivity of children's data in the school system must not be underestimated

3.1 The International Working Group on Data Protection in Telecommunications recognised in its working paper on e-learning platforms (2017) that *"the sensitivity of digitized pupil and student data should not be underestimated"*.

3.2 "*Education happens to be today, the world's most data-mineable industry by far,*" said the then CEO of Knewton, José Ferreira, in 2012 at the White House Datapalooza. Technology investment is laden with values and the politics of what education means, how and where it is delivered, and who controls it (UNICEF 2018). Estimations of global market value and investments from incubators and angel investors (Metaari 2020) suggest: *"The US accounted for just over 58% ($5.5 billion) of all investments made to learning technology companies in 2017. This changed dramatically in 2018, with companies in China garnering 44.1% of all funding, followed by the US at 32%. This reverted in 2019 with the US retaking their status as the top edtech investment destination. In 2019, China accounted for 'only' 21.4% of all funding on the*

planet while the US accounted for 42.9% of all global funding, double the investments made in China."

3.3 At the same time, under the pressures of keeping costs down and marketisation, the infrastructure to deliver UK state education is exposed to risk via commercial 'freeware' that locks schools into closed, proprietary systems that are run based on platforms that were first developed for business, not children. They often extract children's data and teaching material content with little transparency over processing after transfer from the school, or about their own practices in data analytics (Hessen Data Protection Authority 2019).

3.4 There are regular reports of security problems in apps that process children's sensitive data, such as children's mental health assessments (The Register 2019) yet neither the efficacy nor credentials of apps are required to meet the high bar of necessary due diligence that medical apps might be (NHS 2020). Risks to personal, institutional (BBC 2019), and national security, of both data and technology infrastructures are underestimated in a single school risk assessment, that does not look for national or collective risk.

3.5 The State further creates and controls a child's national digital footprint by their fifth birthday. This creates risks for the child when identifying data from the National Pupil Database are given to thousands of non-state actors (Department for Education, 2020) without a child's or their family's knowledge (Survation poll 2018). Government departments further link and repurpose individuals' education data with their records across government, which adds further levels of sensitivity through its joined-up additional knowledge and impact from use, including use for immigration enforcement (defenddigitalme 2016).

4. Children's rights are failed in practice

4.1 When it comes to a legal basis for data processing as the first protection for children, schools are the gatekeepers not only for the State, but for thousands of third-parties to gain access to millions of children's lives. If the school assumes an absolute right to make choices on the child's behalf, which technology must be used in the classroom or for homework, the most fundamental principles of data protection are easily ignored. Schools routinely assume all data processing is permissible under the public task. But features designed for easy school administration can risk abuse, such as compulsory open directories (The Register 2018). Even where companies' terms and conditions state consent is required, children's personal details,

often together with parents' emails, are routinely extracted in bulk from the core MIS to third-parties, and without parental permission.

4.2 This lack of accountability fails children. Third-parties generally assume that they are data processors not controllers, but may be incorrect where they routinely determine the nature and purposes of processing (defenddigitalme case studies 2020).

4.3 Fundamental principles in data rights include a right to know who collects which personal data about you, for what purposes, who it is shared with, how long it is kept, and rights to correct inaccuracies or object to marketing re-use. All these rights are ignored where the companies pass on the responsibility to the schools that rarely have the understanding or capacity to manage the 'new governmental arrangements' of big data they process (Williamson 2017a).

4.4 Even for special category data such as religion, consent as a legal basis for processing personal data can fail children. A recent national project extracted the personal data including religion and behavioural data from 65,000 children, claiming legitimate interests (Ruda 2019). UCAS, the UK university applicant system asks young people (who may be under 18 routinely in Scotland, or at the time of applying) for consent to share their religion, sexual orientation and disabilities with their future university, as part of the higher education application equality monitoring process. But application forms do not explain that this will be linked with their named, individual national pupil record, and be kept indefinitely at the Department for Education (Shearing 2019).

4.5 Increasingly invasive technology has become normalised in schools, as tools have become routine without challenge. Not only can apps be used to document whole class behaviour, but body worn cameras too. In 2018, a school in Birmingham installed cameras the size of a fifty pence coin in classrooms to monitor voice and movement (Schools Week 2018) for teacher training purposes. How can schools respect individual rights in class-wide policies?

4.6 Commercial exploitation may not be explicit. Apps that monitor children's behaviour scores may have terms and conditions on not reselling data. But they might also require that the school accepts click-wrap agreements - pre-packaged terms and conditions designed by the company that cannot be changed by the school and must be accepted to continue to use the product even if they change over time. Indefinite pseudonymous data retention is routine in such terms. It is also common for companies to re-use personal data for their own commercial purposes; whether for in-app adverts, or to send parents emails for premium products. Families are a captive audience.

4.7 The increasing scale, speed and simplicity of data transfer has been rapid, while data storage cost has fallen. The technological barriers to data access, copying and distribution have been diminished while the complexity of emerging products has grown.

4.8 It is impossible for a school to really understand how lots of these tools work. Researchers at the Oxford University Department of Computer Science, revealed the extent of hidden trackers, in an assessment of nearly one million apps (Binns et al. 2018). And if developers might not even understand the full extent of what their code does (Ekambaranathan et al. 2020), how can schools meet the obligations of data privacy and protection by design and default (ICO 2020a) or teachers be expected to understand all this and explain it to families? All these circumstances create an increase in the need for expert due diligence in order to realise children's rights in practice, that cannot be adequately met in today's school systems.

5. Can regulatory enforcement save us?

5.1 The Data Protection Authority in Sweden was the first decision under GDPR, to recognise the power imbalance in schools, and rule that consent was invalid, in the case of facial recognition used for registering attendance (Swedish Data Protection Authority 2019). In Norway insufficient technical and organisational measures to ensure information security were found in a home school communications app. And in the UK the ICO made an interim statement during its investigation of the Department for Education that the Department breached data protection rules over its controversial pupil nationality data collection and by sharing pupils' details with the Home Office since 2015 (Schools Week 2019). In 2020 its audit made 139 recommendations, of which over 60% were urgent or high priority (ICO 2020b). However, if enforcement is only on a case-by-case basis, will that bring about the systemic change needed to respect children's rights?

5.2 Natasha Singer writing in the New York Times in May 2017, described in her words, how Google took over the US 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."

5.3 Large companies that capture large amounts of personal data about large numbers of children - millions in multiple countries - are growing a power base that other companies simply do not have. It is power that goes beyond data processing but starts to reach into how and what teachers teach. By shaping staff training, you capture elements of the shape of the curriculum and the structure of how it is delivered, at country level, then worldwide. Research is needed to ask whether this shapes a change in not only state delivered education but its purpose — why focus on teacher knowledge after all, if your company has turned its search term to look for knowledge online, into a common verb?

5.4 How transparent are their objectives and with what oversight are their outcomes measured? The potential global implications for the future cost and stability of the state sector education infrastructure, and the individual and collective costs to children in terms of privacy and normalisation may be shaping students and society in ways we are yet to see.

6. Taking stock of system led decision-making

6.1 Artificial intelligence can be used from low-level decision making, such as assigning class seating plans based on children's behavioural scoring through to shaping a personalised curriculum. But although commonly referred to in marketing materials, what AI actually is and does in some tools is vague, *"often indistinguishable from the application of computing, statistics, or even evidence"* (Veale 2019).

6.2 Developers shape what is done to children through their design. There are no statutory boundaries of how far they are permitted to nudge a child's behaviour, how they affect a child's mental health, how they judge a child's performance, how they judge the intent behind a child's Internet search, and what data analytics they 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. These decisions are shaping children's lives.

6.3 The GDPR term 'significant effect' is not yet well enough understood, particularly in terms of future effects on children and predictive us-

es of data and while such effects may not yet be transparent to public sector staff or families. The predictive utility and accuracy of risk factors are largely assumed rather than established via independent evaluation of the tool (Van Brakel 2019). Others have also proposed children must be better protected from such technology using historical data: "*Children should be ensured a free, unmonitored space of development, and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data*" (HLEG-AI 2019).

7. What is next?

7.1 The next generation of technologies is already intervening in the lives of the next generation of society in ways that we do not yet understand. We are failing to ask the right questions of policy makers and companies. We are allowing the available tools to shape education unquestioningly when the hype of edTech achievement so far outweighs the evidence of delivery. Writing in the Impact magazine of the Chartered College in January 2019 Neil Selwyn summed up:

> *"the impacts of technology use on teaching and learning remain uncertain. Andreas Schleicher – the OECD's director of education – caused some upset in 2015 when suggesting that ICT has negligible impact on classrooms. Yet he was simply voicing what many teachers have long known: good technology use in education is very tricky to pin down*."

7.2 Behavioural science, neuroscience (Standaert 2019), psycho-policies (Williamson 2017b), personalisation through genetics (Education Select Committee 2013), facial recognition and gait analysis, affective tech (Nemorin 2017), and questions over the use of other emerging technologies including using AI in school surveillance software for countering-violence and extremism (defenddigitalme 2019) abound. In the face of these advances, and in the volume and velocity of data processing, there is an urgent need to support moratorium (Kaye 2020) while the exercise of rights is enabled in practical and meaningful ways.

8. Conclusion: How do we build a rights-respecting environment for life not just one day?

8.1 Data protection alone is insufficient to protect children's full range of rights in the digital environment. Only by reshaping the whole process,

will we have a chance to restore the power balance to schools and to families. Schools must return to a strong position of data controllers and delegate companies to data processors with consistent standards on what they are permitted to do. That infrastructure may not exist, but we need to build it.

8.2 Procurement processes must require assessment of what is pedagogically sound and what is developmentally appropriate, as part of risk assessment including data protection, privacy and ethical impact. Assessment of risk is not a one-time state at the start of data collection, but across the data life-cycle. While teacher training must include a core requirement on data and digital rights, and continuing professional development should be offered regularly, a shared-skill model could reduce the burden of due diligence across every school.

8.3 Legislation, Codes of Practice, and enforcement need to prioritise the full range of human rights of the child in education, in accordance with COE Recommendation CM/Rec (2018) of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, and the Council of Europe (2020) Committee on Convention 108 Guidelines on Children's Data Protection in an Education Setting. Policy at all levels 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:

> *"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."*

8.4 Consent and contract terms must be rethought in the context of education. As set out by the European Data Protection Board in 2020 *Guidelines on consent*, children [and their guardians] cannot freely consent to data processing, where the nature of the institutional-personal power imbalance means that consent cannot be refused, or easily withdrawn without detriment, and they recognise that the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.

8.5 Defining standards and expectations could begin in data security, set out in statutory Codes of Practice (Art. 40 GDPR) and Freedom of Infor-

mation laws should be applied to all non-state actors, companies and arms´ length government bodies, providing education and children's services to the publicly funded state sector.

8.6 Public Authorities should document and publish

- commercial processors /subprocessors engaged in children's data processing
- a register of any commercially obtained sources of personal data collected for processing, or linkage with data provided by individuals in the course of their public sector interactions (Dencik et al 2019), and update it on a regular basis (i.e., Data brokers, third-party companies, social media).
- Data Protection Impact Assessments, Retention schedules, and GDPR s36(4) Assessments with periodic reviews to address change.

8.7 Sector-wide changes are needed on

- Children's agency
- The role of families
- The role of school staff
- A model framework of management of permitted processing not based on consent
- Reducing the investigative burden
- 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.

8.8 An alternative model of data rights' management in education is that of the U.S., governed by FERPA with state variations. It is imperfect but offers a regional model of law and expertise for schools to rely on, with trusted contractual agreements. Schools are data controllers. Processors cannot change terms and conditions midway through the year, without agreed notifications, and reasonable terms of change. Families get a list each year (or at each school move) to explain the products their child will be using - and crucially, legal guardians retain a right to object. 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 (Student Privacy Compass).

8.9 A strong foundation must be built to ensure children do not lose their human rights by virtue of passing through the school gates. While the UK government is driving an edTech strategy for post-Brexit export, it fails to address fundamental principles of data laws, and the child rights framework needed for the safe use of educational products, not only in the life of a child on one day, but forever.

References

Adams, Richard (2018): *Student Loans Firm Accused of 'KGB Tactics' for Assessing Eligibility.* In: The Guardian. Online verfügbar unter: https://www.theguardian.com/education/2018/oct/30/student-loans-firm-accused-of-kgb-tactics-for-assessing-eligibility [Abfrage am: 6.10.2020].

Allen-Kinross, Pippa (2019): *DfE Facing Action Iver 'Wide Ranging and Serious' Data Protection Breaches*. In: Schools Week. Online verfügbar unter: https://schoolsweek.co.uk/dfe-facing-action-over-wide-ranging-and-serious-data-protection-breaches/ [Abfrage am: 4.10.2020].

Binns, Reuben / Lyngs, Ulrik / Van Kleek, Max / Zhao, Jun (2018): *Third Party Tracking in the Mobile Ecosystem*. Online verfügbar unter: https://www.researchgate.net/publication/326138940_Third_Party_Tracking_in_the_Mobile_Ecosystem [Abfrage am: 6.10.2020].

Chirgwin, Richard (2018): *Victoria's Educational Apps-For-Students Let Creeps Contact Kids*. In: The Register. Online verfügbar unter: https://www.theregister.co.uk/2018/05/22/has_google_built_a_haven_for_creeps_in_victorias_education_apps/ [Abfrage am: 4.10.2020].

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*. Online verfügbar unter: https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf.

Corfield, Gareth (2019): *Pupil Mental Health Monitor Promises App Rewrite After Hardcoded Login Creds Discovered*. In: The Register. Online verfügbar unter: https://www.theregister.co.uk/2019/09/27/pupil_mental_health_tracking_app_security_fears/ [Abfrage am: 4.10.2020].

Coughlan, Sean (2019): *Hackers Beat University Cyber-Defences in Two Hours*. In: BBC. Online verfügbar unter: https://www.bbc.co.uk/news/education-47805451 [Abfrage am: 4.10.2020].

Council of Europe (2020): Committee on Convention 108 *Guidelines on Children's Data Protection in an Education Setting* https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting- [Abfrage am: 27.11.2020]

Defenddigitalme (2016): *Timeline of Home Office Access to Pupil Data in England for Immigration Enforcement*. Online verfügbar unter: https://defenddigitalme.org/timeline-school-census/ [Abfrage am: 6.10.2020].

Defenddigitalme (2018): *A Comparison of National Pupil Databases in the UK*. Online verfügbar unter: http://defenddigitalme.com/wp-content/uploads/2018/03/UK_pupil_data_comparison-1.pdf [Abfrage am: 6.10.2020].

Defenddigitalme and Survation (2018): *The State of Data 2018. A Poll of 1,004 of Children Aged Five to Eighteen, in the State Education System*. Online verfügbar unter: https://defenddigitalme.com/stateofdata2018-gdpr/ [Abfrage am: 6.10.2020].

Defenddigitalme (2020) Case studies: *The State of Data 2020: mapping a child's digital footprint across state education* (Report section 3.8.4) https://defenddigitalme.org/state-of-data/ (Abfrage am 07.10.2020)

Dencik, Lina / Hintz, Arne / Redden, Joanna / Warne, Harry (2018): *Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services.* Data Justice Lab, Cardiff University, UK. Online verfügbar unter: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf [Abfrage am: 6.10.2020].

Denham, Elisabeth (2017): *The Information Commissioner Findings on Google DeepMind and Royal Free*. Online verfügbar unter: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/ [Abfrage am: 6.10.2020].

Department for Education (DfE) (2020): *External Data Shares*. Online verfügbar unter: https://www.gov.uk/government/publications/dfe-external-data-shares [Abfrage am: 6.10.2020].

European Commission (2019): *High-Level Expert Group on AI (AI HLEG) Policy and Investment Recommendations for Trustworthy Artificial Intelligence*. Online verfügbar unter: https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence [Abfrage am: 6.10.2020].

European Data Protection Board (2020): *Guidelines on Consent Under Regulation 2016/679*. Online verfügbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Abfrage am: 6.10.2020].

Education Select Committee (2013): *Underachievement in Education by White Working Class Childr*en - para 77. Online verfügbar unter: https://publications.parliament.uk/pa/cm201415/cmselect/cmeduc/142/14206.htm#a38 [Abfrage am: 6.10.2020].

Ekambaranathan, Anirudh / Zhao, Jun / Van Kleek, Max (2020): *Understanding Value and Design Choices Made by Android Family App Developers*. In: CHI'2020. Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA, S. 1-10.

Ferreira, Jose (2012): *CEO of Knewton, Speaking at the DataPalooza on the U.S. Department of Education YouTube Channel of the Office of Educational Technology*. Online verfügbar unter: https://youtu.be/Lr7Z7ysDluQ [Abfrage am: 6.10.2020].

Hessen Data Protection Authority (2019): *Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen.* Opinion on the Use of Cloud Storage like Amazon, Google, Microsoft 365 in State Schools under GDPR. Online verfügbar unter: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und [Abfrage am: 6.10.2020].

ICO (2020a): *On Article 25 Data Protection by Design and Default*. Online verfügbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Abfrage am: 6.10.2020].

ICO (2020b): *Statement on the outcome of the ICO's compulsory audit of the Department for Education.* Online verfügbar unter: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/ (Abfrage am 07.10.2020)

Kaye, David (2019): *Moratorium Call on Surveillance Technology to End 'Free-for-All' Abuses: UN Expert, Recommendations*. In: UN News. Online verfügbar unter: https://news.un.org/en/story/2019/06/1041231 [Abfrage am: 6.10.2020].

Leaton Gray, Sandra / Phippen, Andy (2017) *Invisibly Blighted: The Digital Erosion of Childhood.* London: IOE Press.

Lupton, Deborah / Williamson, Ben (2017)*: The Datafied Child: The Dataveillance of Children and Implications for Their Rights*. In: New Media & Society 19(5), S. 780-794. Online verfügbar unter: https://doi.org/10.1177/1461444816686328 [Abfrage am: 6.10.2020].

Metaari (2020): *Global Edtech Investments Reach a Staggering $18.66 Billion via PRweb*. Online verfügbar unter: https://www.prweb.com/pdfdownload/16814926.pdf [Abfrage am: 6.10.2020].

Murray, Cath (2018): *A Camera in Every Classroom: Would You Do It?* In: Schools Week. Online verfügbar unter: https://schoolsweek.co.uk/a-camera-in-every-classroom-would-you-do-it/ [Abfrage am: 4.10.2020].

Nemorin, Selena (2017): *Affective Capture in Digital School Spaces and the Modulation of Student Subjectivities*. In: Emotion, Space and Society 2, S. 11-18.

NHS (2020): *Apps Library 'How the Assessment Works'*. Online verfügbar unter: https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools#how-the-assessment-works.

Ruda, Simon (2019): *BIT Director of Home Affairs and International Programmes* (at 1:36) "Imminently we will be launching a trial with 75 schools and 65,000 children...". Online verfügbar unter: https://www.youtube.com/watch?v=z2Vvt8wK-gYU [Abfrage am: 6.10.2020].

Selwyn, Neil (2019): *Teachers and Technology: Time to Get Serious.* In: Journal of the Chartered College. Online verfügbar unter: https://impact.chartered.college/article/editorial-education-technology/ [Abfrage am: 6.10.2020].

Shearing, Hazel (2019): *Millions Of Students' Sexual Orientations And Religious Beliefs Are Being Held On A Government Database.* In: Buzzfeed UK. Online verfügbar unter: https://www.buzzfeed.com/hazelshearing/the-government-has-a-database-of-millions-of-students [Abfrage am: 6.10.2020].

Singer, Natasha (2017): *How Google Took Over the Classroom*. In: The New York Times. Online verfügbar unter: https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html [Abfrage am: 6.10.2020].

Standaert, Michael (2019): *Chinese Primary School Halts Trial of Device that Monitors Pupils' Brainwaves*. In: The Guardian. Online verfügbar unter: https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves [Abfrage am: 4.10.2020].

Stoilova, Mariya / Livingstone, Sonia / Nandagiri, Rishita (2019): *Children's Data and Privacy Online*. Online verfügbar unter: https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf [Abfrage am: 6.10.2020].

Student Privacy Compass (2020): *Named After the Core Federal Law that Governs Education Privacy, FERPA, This is a U.S. Education Law and Privacy Resource Site*. Online verfügbar unter: https://studentprivacycompass.org/state-laws/ [Abfrage am: 6.10.2020].

Swedish Data Protection Authority (2019): *Supervision Pursuant to the GDPR (EU) 2016/679 –[DI-2019-2221] Skellefteå Municipality*. Online verfügbar unter: https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf [Abfrage am: 6.10.2020].

Taylor, Emmeline (2019): T*eaching Us to Be 'Smart'? The Use of RFID in Schools and the Habituation of Young People to Everyday Surveillance*. In: Taylor, Emmeline / Rooney, Tonya (Hg.): Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People. Emerging Technologies, Ethics and International Affairs. Oxon / New York: Routledge, S. 67-78.

UNICEF (Child Rights and Business Unit) (2018): *Discussion Paper Series: Children's Rights and Business in a Digital World. Privacy, Protection of Personal Information, and Reputational Rights*. Online verfügbar unter: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf [Abfrage am: 6.10.2020].

Van Brakel, Rosamunde (2019): *Rise of Pre-Emptive Surveillance: Unintended Social and Ethical Consequences*. In: Taylor, Emmeline / Rooney, Tonya (Hg.): Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People. Emerging Technologies, Ethics and International Affairs. Oxon / New York: Routledge, S. 187-199.

WhatDoTheyKnow (2018): *FOI Reference: 4368666 A Freedom of Information Request from Jen Persson to Kent County Council Integrated Dataset: Children and Young People*. Online verfügbar unter: https://www.whatdotheyknow.com/request/integrated_dataset_children_and_4 [Abfrage am: 6.10.2020].

Williamson, Ben. (2017a): *Big Data in Education: The Digital Future of Learning, Policy and Practice*. London: Sage.

Williamson, Ben (2017b) *Decoding ClassDojo: Psycho-Policy, Social-Emotional Learning and Persuasive Educational Technologies, Learning, Media and Technology,* 42 (4), S. 440-453. Online verfügbar unter: https://doi.org/10.1080/17439884.2017.1278020.