The Right to Privacy (Article 8) and the Digital Revolution inquiry

Written evidence from defenddigitalme

1. Executive summary

1.1 The state education system creates and controls a child's digital footprint by their fifth birthday, and gives it away to thousands of commercial companies by distributing pupils' personal confidential data; often without a child or their family's knowledge or consent.

1.2 Across the UK, state education is deeply entwined with, and dependent on, digital tools. Direct data collection by commercial companies begins in pre-school and it may be hard to appreciate how datafied a child is, as a result of state education, by age 19. (See Annex A)

1.3 Harms to children's privacy, dignity, free expression, and their UNCRC rights to full development and human flourishing, can result from various areas of commercial practice. The accountability system, software used for safeguarding, behavioural surveillance, testing, admin, and by data mining the 'datafied child.'[1] The implications for the child and society are staggering. In the words of two global education companies CEOs':

"Privacy went out the window in the last five years. For the good of society, for protecting kids."

School safeguarding software company Gaggle CEO, Jeff Patterson (2019)[2]

"the human race is about to enter a totally data mined existence, and it's going to be really fun to watch...the world in 30 years is going to be unrecognisably data mined...education happens to be today, the world's most data mineable industry– by far."

Educational Platform Knewton (now Wiley) former-CEO, Jose Ferreira (2012)[3]

1.4 For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the $8bn global edTech market[4], propagated not only by angel investors and tech accelerators in US and UK[5] English language markets, but across the world.

1.5 At the same time, under the pressures of austerity and marketisation, the infrastructure to deliver UK state education is exposed to risk via commercial 'freeware'. There is pressure to use benchmarking data analytics, pool pupil data into data lakes, and link student data in Higher Education[6] with other government departments' data (HMRC, DWP). The potential implications for the security and stability of the state sector education infrastructure, the costs to privacy, and effects of normalisation, may last a lifetime for this datafied generation.

1.6 As Lupton and Williamson pointed out in 2017,

> ***"Children are becoming the objects of a multitude of monitoring devices that generate detailed data about them, and critical data researchers and privacy advocates are only just beginning to direct attention to these practices."***

[1] Lupton, D. and Williamson, B. Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780–794. https://doi.org/10.1177/1461444816686328 (ibid reference in paragraph 1.6)

[2] *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming*, Education Week (July 8, 2019) reporting from interview with school safeguarding software Gaggle CEO Jeff Patterson https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html

[3] Quotes source: YouTube channel of the Office of Educational Technology at the US Department of Education. https://www.youtube.com/watch?v=Lr7Z7ysDluQ Knewton, an adaptive learning company that has developed a platform to manage educational content, has developed courseware for higher education https://www.knewton.com/ It was bought by Wiley in 2019.

[4] UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World (p5) Privacy, Protection of Personal Information, and Reputational Rights https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

[5] EDUCATE https://educate.london/

[6] Dr Ben Williamson, University of Edinburgh, Centre for Research in Digital Education and the Edinburgh Futures Institute. Big Data in Education, the digital future of learning, policy and practice (Sage) (2017)

2. Recommendations

2.1 We would welcome legislation, statutory Codes of Practice, and enforcement action to protect the full range of human rights of the child and young people in the digital environment in education.

2..1.1 Researchers at LSE in 2019 have documented how children care about their privacy online, that they want to be able to decide what information is shared and with whom,[7] and further that, *"teachers are unclear what happens to children's' data and there is common misunderstanding of how much data leaves a school:",*

> *"The only time it does [to the government] is when we do the Year 11 data [...] Because obviously they'll do the tracking of different groups. (teacher, London)"*

2.1.2 and when it comes to using educational platforms, *"I would've thought the fact that it's a school-based software, this is all been properly regulated." (teacher, London)"*

2.2 Prioritise privacy in the rights of the child in the digital environment across the public sector.

2.2.1 Incorporate the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment across the public sector.

2.2.2 The current consultation on a *national data strategy*[8] must take a rights based approach ahead of the want to '*unlock the power of data across government and the wider economy.*' While DCMS asks for views on trust on use, it does not seek to address rights around collection and retention. This prevailing attitude and approach contravene the second principle of data protection law on purpose limitation. 'Now we've got it, how can we use it?' style thinking should end, not expand, and needs enforcement of data protection law.

2.2.3 Young adults must have a right to obscurity, and not feel obliged to be surveilled simply by participating in education or find that their personal data are repurposed for other uses by default, such as general monitoring to infer mental health. The latest Office for Students' projects are invasive[9], and JISC's social media post on the plan talked of '*data harvesting.*'[10] In June 2019, Paul Feldman[11] the CEO of Jisc said during a talk on Higher Education data analytics that the extent of the Jisc data surveillance, tracking and profiling meant that,

> "*we [JISC] can track them around campus, though that gets quite freaky and they object to some of that*."(end quote)

2.2.4 This goes against what students said they wanted in response to a 2015 UCAS survey of applicants[12]. From a total of 37,000, 90% of respondents supported sharing their personal details outside of the admissions process "*only with active and informed consent".*

---

[7] Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age, http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[8] National Data Strategy open call for evidence (June 2019) https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence/national-data-strategy-open-call-for-evidence#questions

[9] Innovation, partnership and data can help improve student mental health in new £14m drive https://www.officeforstudents.org.uk/news-blog-and-events/press-and-media/innovation-partnership-and-data-can-help-improve-student-mental-health-in-new-14m-drive/

[10] "Identifying students in crisis by harvesting data on individuals" https://twitter.com/PaulbernalUK/status/1136275932950536192 *Universities to trawl through students' social media to look for suicide risk, under new project,* Telegraph, June 5 2019, https://www.telegraph.co.uk/education/2019/06/04/universities-trawl-students-social-media-look-suicide-risk-new/

[11] Paul Feldman, CEO Jisc, June 2019 https://www.hefestival.com/speakers-2019/paul-feldman-2/ Panel event 12.20-13.10: *Artificial Intelligence: Robotics, the curriculum and inclusion* https://www.hefestival.com/programme-2019/

[12] UCAS (October 2015) *37,000 students respond to UCAS' Applicant Data Survey* https://www.ucas.com/corporate/news-and-key-documents/news/37000-students-respond-ucas%E2%80%99-applicant-data-survey

2.2.5 The government should ensure effective implementation of their obligations under Article 13 of the European Convention on Human Rights, and other international and human rights instruments, to fulfil a child's right to an effective remedy when their human rights and fundamental freedoms (such as Article 8) have been infringed in the digital environment.

2.3 Level-up legislation to protect the privacy rights of the child across the UK

2.3.1 Level up the safeguards on commercial re-use of national pupil data across the four[13] UK national pupil databases, used by third parties after release by government.

2.3.2 Enforcement of lawful bases for children's personal data in education. For example, most apps' terms and conditions set out, that they process on the basis of consent. But as set out by the ICO, children cannot freely consent to the use of such services in particular where the power imbalance is such that it cannot be refused, or easily withdrawn. "*Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent."* There are also problems with child/parental consent.

2.3.3 Ensure high standards of consumer protection, privacy, and data protection laws are applied to educational apps and platforms consistently across the UK.

2.3.4 Biometric data are processed by commercial companies and *the Protection of Freedoms Act 2012* applies only to schools in England. Introduce legislation on protections of biometric data in Northern Ireland and Scotland consistent with England and Wales, required across the UK to protect and fulfil the rights of the child in the digital environment across the public sector. In other countries use of biometrics is not permitted for children.

2.3.5 Subject access rights should be standardised for children across all schools in the UK to change the inconsistency between Local Authority and academy/free school models of support of parental and child rights to subject access and access to the educational record and the wide variety of school information management systems (stored in schools or offsite on companies' cloud servers which are commonly abroad[14]), platforms and apps in use.

2.4 Increase transparency of commercial use and reuse of children's personal confidential data to families themselves

2.4.1 An independent audit should take place of the commercial reuse of children's personal confidential data from national pupil data, distributed at all national levels.

2.4.2 Obligations should be made on controllers and processors of biometric data to have a duty to explicitly register processing biometric data with the ICO where it concerns a child.

2.4.3 Freedom of Information laws should apply to all companies and arms length government bodies, providing education and children's services to the UK public sector.

2.4.4 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[15] , and update it on a regular basis. (i.e. Data brokers, third-party companies, social media)

[13] A comparison of national pupil databases in the UK composed by defenddigitalme http://defenddigitalme.com/wp-content/uploads/2018/03/UK_pupil_data_comparison-1.pdf

[14] The German Data Protection Authority in Hessen is of the opinion that the use of cloud storage like Amazon, Google, Microsoft365 in state schools is illegal under the GDPR because of US jurisdiction issues. It found that processing is opaque and data trails not been explained in ways that can be understood, so schools cannot demonstrate DP compliance. https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und

[15] Cardiff Data Justice Lab Data Risk Scores https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf

- Data Protection Impact Assessments, Retention schedules, and GDPR s36(4) Assessments with periodic fixed review to address changes

2.5 Improve the clarity, confidence and consistency in lawful data processing across schools for staff and families

2.5.1 A statutory Code of Practice in education would underpin and enforce good practice, bringing clarity, consistency and confidence to data handling across the sector.

2.5.2 Initial teacher training must start to include a core requirement on data and digital rights, and similarly CPD should be offered regularly to teachers and school staff.

2.5.3 Standardisation of data privacy and protection policies for schools should be supported at national level and seek to reduce the number of policies given to parents on admissions. These often come as thirty separate, multi-page documents, and third-party commercial companies are commonly left out of explanations in privacy notices and retention schedules.

2.6 Limitations on exploitation and restrictions are needed on high risk technology, and research in school settings, to be appropriate to children

2.6.1 Consider legislative limitations of surveillance via various biometrics, facial detection and recognition, emotional manipulation, and neuro-/cognitive technology by commercial companies, or via webcam, voice recording, or gait and movement analysis, noting UN Special Rapporteur David Kaye's call for a moratorium on facial recognition technology[16] .

2.6.2 Webcams should never be used in education to take a photograph of a child using a computer, without their knowledge or permission, or their use of the Internet monitored at home, as happens today in England through use of safeguarding-in- schools software. Legislative protection and policy change are needed to accompany the existing weak statutory guidance in England for school pupil web surveillance vendors, to assist schools to comply with the Data Protection Act 2018, human rights law and end the serious problems with policy, and the invasions into private and family life that exist today.[17]

2.6.3 Pupils and students must be free from any obligation of using personal profiles and accounts on social media[18], and to avoid privacy risks, separate group and personal accounts, and more broadly, limit their use for school communications and administration.

2.6.4 Artificial intelligence companies should not exploit children's data gathered in the course of compulsory education, for their own company product development.

2.6.5 Behavioural science, neuroscience, personalisation via genomics, facial recognition and gait analysis, nudge, affective tech[19], and other emerging technologies should not be trialled in schools. Any research studies should require ethical oversight and opt in consent.

2.7 Historical data collections need enforcement for current respect of human rights and data protection law

2.7.1 The Department for Education in England is aware that they share too much data with third party users, calling it an '*excessive' amount of data in the underlying datasets'*.[20]

---

[16] Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert
, (June 2019) David Kaye recommendations, United Nations Special Rapporteur on freedom of opinion and expressionhttps://news.un.org/en/story/2019/06/1041231

[17] Defenddigitalme, working briefing on web monitoring in use for management of online harms and 'safeguarding in schools' https://defenddigitalme.com/wp-content/uploads/2019/07/AP-Copy-V1.6-Working-Copy-of-DRAFT-WIP_-Web-Monitoring-Briefing-defenddigitalme.pdf

[18] The Education Foundation, (Goddard. T, and Fordham, I.) Facebook Guide for Educators (2013) http://www.ednfoundation.org/2013/06/21/facebook-guide-for-educators/

[19] Dr Selena Nemorin, University College London, Affective capture in digital school spaces and the modulation of student subjectivities. Emotion, Space and Society, 24. pp. 11-18. ISSN 1755-458

[20] DfE data dissemination discovery report, 2018 (p29)

2.7.2 The state must address the requirements under the Data Protection Act 2018 (and GDPR Article 25[21]) to minimise its data collections and ensure proper policy, technical and security measures to address excessive data collection and enforce retention (including at national levels on leaving school), limit unique identifiers, and ensure anonymisation.

2.7.3 Children's data must not be used for purposes incompatible with the one that legitimised their collection and that the people were told about at that time. Non-educational purposes of national pupil data by other government departments (Home Office) must end.[22]

2.7.4 Explore a non-commercial-use duty on data collected prior to changes of 2012 law.

2.7.5 It is common for edTech to re-use personal data provided for the school / pupil's purposes of direct admin, teaching or communications,, for their own commercial company purposes; whether for in-app advertising, pitching at parents' emails for upgraded or sister products, or product development including new AI tools; chat bots, and virtual learning platforms. Children and their parents being captive addressees for marketing is mainly a consumer protection problem. But from a human rights point of view, it is the prior collection of personal data, and repurposing for indirect uses, which is problematic for privacy. Further uses of compulsory [access][23] data, misused to restrict 'undesirables', is already a reality.

2.76 Children must have a right to restriction of disclosure to private companies to ensure their full development and adult flourishing. It should be possible for school records with behavioural history to be suppressed from distribution; records such as violence, sexual misconduct, or drugs, if criminal would be suppressed under the Rehabilitation of Offenders Act 1974; but as **non**-criminal records, may be passed on for life to third parties, without a child's (or their later adult) knowledge, and may be sent to the US or other jurisdictions.

2.8 Lawmaking[24] and procurement at all levels of government must respect the UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights[25]

2.8.1 *"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****."*

2.9 Machine learning and AI using pupil data, automated decision making, profiling, risk scores and prediction, must all have tight oversight across their lifetime use, and be understandable to public sector staff and families.

2.9.1 In June 2019, the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their Policy and Investment Recommendations for Trustworthy Artificial Intelligence, proposed children must be better protected when used with such technologies.

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721729/HiveIT_-_DfE_dissemination_discovery.pdf

[21] ICO Data Protection by Design and Default (Article 25)
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/

[22] Timeline of Home Office access to pupil data in England for immigration enforcement purposes
https://defenddigitalme.com/timeline-school-census/

[23] King's College London has apologised to student activists who were barred from entering the university's buildings during a visit by the Queen in March, after an inquiry found security staff "overstepped their authority".
https://www.theguardian.com/education/2019/jul/04/kings-college-security-overstepped-authority-over-activists-during-queens-visit-inquiry

[24] Higher Education and Reserch Act 2017 and Regulations 2018/19
https://www.parliament.uk/documents/lords-committees/Secondary-Legislation-Scrutiny-Committee/Session%202017-19/Product%20safety/Defenddigitalme%20submission%20on%20%20Higher%20Education%20Act%20Regulation%202019%20v2.pdf

[25] Committee on the Rights of the ChildGeneral comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

> "*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.*"[26]

2.9.2 There need be no conflict between privacy and innovation[27], yet some products in emerging fields, including machine learning and Artificial Intelligence infringe on rights.

2.9.3 In 2017 Wired magazine[28] revealed that the government's 'Nudge Unit' or the Behavioural Insights Unit had been experimenting with using machine learning algorithms to rate how well schools were performing, and they were opaque by design:

> "*Data on student's ethnicity and religion were deliberately excluded from the dataset in an effort to prevent algorithmic bias. Although some factors will influence the algorithm's decision more than others, Sanders refused to say what those factors where. This is partly because he doesn't want schools to know how the algorithm makes its decisions, and partly because it is difficult to know exactly how these algorithms are working, he says. "The process is a little bit of a black box – that's sort of the point of it," he says.*

2.9.4The hype of 'edTech' achievement in the classroom so far, far outweighs the evidence of delivery. Neil Selwyn, Professor in the Faculty of Education, Monash University, Australia, writing in the Impact magazine of the Chartered College in January 2019 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.*"[29]

2.9.5 There is no way for school children, students or their families to be fully aware of how their data are being used, and in the course of state education they have no meaningful choice or control over data processing. We believe few staff in institutions across the state education sector, providing services to children age 2-18, have adequate grasp of this either. This is a poor foundation for the expansion of an edTech strategy DfE has begun in 2019.

2.9.6 A stronger foundation must be built first including data usage reports for children and families to know '*who knows what about me',* Data privacy and protection must be introduced as part of basic teacher training and into compulsory CPD, and regulation of current policy and practice as set out (2), should begin through consultation.

For the sake of brevity we include some of our research separately in Annexes

A) A graphic to demonstrate "one day in the life of a datafied child" in school in England.
B) What do we mean by personal data in education
C) National pupil database distribution by DfE for commercial re-use by third party companies[30]
D) Higher Education: Expansion of commercial re-use by data analytics companies
E) The approved and declined range of commercial tools used in one Local Authority in Scotland,

We are happy to answer any questions the Committee may have.
Defenddigitalme,

---

[26] Policy and Investment Recommendations for Trustworthy Artificial Intelligence (accessed July 1, 2019) (published June 26, 2019) https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (permanent copy https://defenddigitalme.com/wp-content/uploads/2019/07/AIHLEGPolicyandInvestmentRecommendationspdf.pdf)

[27]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/ Denham, E., The Information Commissioner3 July 2017, findings on Google DeepMind and Royal Free

[28] Reynolds, M., Wired, December 2017, *UK's Nudge Unit tests machine learning to rate schools and GP https://www.wired.co.uk/article/nudge-unit-machine-learning-algorithms-schools-ofsted-doctors-behavioural-insights*

[29] Neil Selwyn, Monash University Australia, writing in the Impact magazine of the Chartered College, (January 2019) https://impact.chartered.college/article/editorial-education-technology/

[30] DfE external data shares https://www.gov.uk/government/publications/dfe-external-data-shares

July 2019

About defenddigitalme

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. We advocate for children's data and digital rights, in response to concerns about increasingly invasive uses of children's personal information. The campaign is funded by an annual grant from the Joseph Rowntree Reform Trust Ltd.