Children and the Internet
House of Lords Communications Committee Consultation

About defenddigitalme

Defenddigitalme is a volunteer non-profit campaign group for children's privacy rights formed in 2015 in response to concerns from parents and privacy advocates about increasingly invasive uses of children's personal data. The campaign asks the Department for Education (DfE) to change their policies and practices to protect 20 million children's identifiable personal and confidential data in the National Pupil Database (NPD):

- stop giving out identifiable personal data to commercial third parties and press without consent
- start telling school staff, pupils, and parents what DfE does with individuals' personal data
- be transparent about policy and practice

More information: http://defenddigitalme.com/

Summary

Our submission responds to the consultation two-part statement that, 'data protection poses a problem for children':

"There is a risk that their personal data may be collected or transferred without them being aware. There is also concern that the online activity of children may remain visible to future employers or academic institutions."

We focus on two areas of the State's collection and use of children's personal and education data which need attention:

I. Secondary uses of children's personal confidential data collected in schools and provided under statutory obligation to the Department for Education:

A. The Department for Education release of these data to third parties.
B. Privacy notices' failure to effectively communicate an understanding of the use and effects of personal data to data subjects, in particular to children, their inadequacy, and derived lack of Data Controller accountability.
C. Subject Access Request rights
D. Public awareness and attitudes towards the National Pupil Database

II. Surveillance of children's use of the Internet and collection of personal data through third party software as part of a Department for Education web monitoring statutory requirement, effective September 5, 2016

A. Web monitoring through third party software
B. Biometrics in schools and personal data collection
C. App surveillance tools and online data collection

Department for Education data policy, practice, and children's rights about the use of confidential data

1. Recent amendments to the Department for Education (DfE) data policy and practice, as well as changes that will shortly impose statutory web surveillance, affect children across all State education, age 2-19 in England. These changes have been characterised by lack of transparent due diligence, public engagement, or democratic debate before imposing significant policy with far reaching potential, and that encroach on children's rights.

2. Data policy and practice about children's confidential data at the Department for Education since 2012, impinge on principles set out in the United Nations Convention on the Rights of the Child, Article 12, *the right to express views and be heard in decisions about them* and Article 16 *a right to privacy and respect for a child's family and home life*. Similar rights that are included in the common law of confidentiality, Article 8 of the Human Rights Act 1998 incorporating the European Convention on Human Rights Article 8.1 and 8.2 *that there shall be no interference by a public authority on the respect of private and family life that is neither necessary or proportionate*, and Data Protection Act 1998, that *data must be processed fairly and for limited purposes, relevant and not excessive, and kept securely for no longer than necessary*. Judgment of the Court of Justice of the European Union in the Bara case (C−201/14) (October 2015) reiterated the need for public bodies to fairly process personal data before transferring it between themselves.[1] The EU

[1] *Judgment of the Court of Justice of the European Union in the Bara case (C−201/14) http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf*

Charter of Fundamental Rights[2], Article 52 also protects the rights of individuals about data and privacy and Article 52 protects the essence of these freedoms. These are fundamental rights that help children develop, and grow. This encroachment into rights has come about over time and incremental scope creep through legislative changes since 2000.

3. We would like to suggest a legislative review of the National Pupil Database with respect to children's rights because technological change in those sixteen years has outstripped the capacity of laws to keep up, and keep pupil data safe. What was designed to enable public benefit from pupil data, has resulted in what the public perceives as misuse of their personal data, namely having been obliged to provide data for a service (their child's education) those same data are being used for purposes far beyond what parents and pupils think reasonable and fair.

Data handling of children's confidential data at the Department for Education

4. Exploiting personal data from individuals for short term economic well-being in the name of the public interest, must not be at the long term expense of societal benefit which can be gained from trusted use of public data.

   Public benefit has been the key purpose of using data in academic research and used to address 'some of the most pressing challenges facing society,' (ESRC, 2016) for a number of years. However recent legal and policy changes in who can access education data and what they can use it for, have expanded the scope of use to exploitation of data beyond the Public Interest to also mean commercial users and individual companies, charities and the press.

5. It is this disparity between government departments and safe research data handling infrastructures, which means inconsistent policy and practices exist in parallel. Secure handling is key to public trust, poor policy and practices jeopardise this and risk data misuse and potential resulting harm.

6. The uses of data by different types of user today are accessed via different pathways, and it is perhaps surprising that the use of the most sensitive individual identifiable data is made via the least safe method and techniques today, opened up to non-safe accredited researchers. There are a number of concerns around the differences between risk level of data release by the Department for Education internal process (DMAP) and identifiable data use outwith any oversight, and without audit and transparency after its release into the wild, which are mitigated by the use of the physical infrastructure of safe settings, safe data practices following UKAN anonymisation techniques, and accreditation of safe researchers. Principles that enable safe and trusted public interest research using population-wide data for the purposes of public benefit, with transparent oversight and outputs, but which the Department practices do not follow.

Expanding the scope of children's confidential data use beyond Education

7. The future scope of children's data to be collected and who these data may be shared with, is about to expand. New Department for Education policy starting in the 2016-17 academic year will increase the volume of individual-level personal data to be extracted to the national database and include country-of-birth, and nationality. There is no legislative difference that will mean these data items would be treated any differently from current use, including other government departments.

8. The government-wide 'datasharing' of all public data is set out in the Digital Economy Bill 2016, will use more identifiable data for a wider range of purposes, and also expand its use in deidentified research or statistical outputs, together with increasing the use of data that have been linked with multiple datasets across different sources.

9. The upcoming Digital Economy Bill 2016 as it is now, comes with a risk that parts of the bill around the use of further expanding scope use of identifiable data by government are likely to result in further unexpected outcomes for children and young people as individuals from unseen data processing in the areas of debt collection such as student loans, and targeted public services (i.e. 'Troubled Families') from stigmatisation from application, or where 'freedoms, rights, or interests' of the individual are contrary to those of 'the State'.

Public voice and expectations about their personal data entrusted to Government

10. We submit evidence of public opinion, the qualitative and narrative responses we have gathered over the course of 2015-16 about public awareness of how personal and education data gathered in school are used by the State, through the National Pupil Database. And we reference the extended public engagement work of the ESRC, Wellcome, and the 2010 Royal Society of Engineering with 14-19 year olds. Our work to date shows young people, parents and school staff are surprised by uses of children's data from the National Pupil Database, especially by commercial use.

---

[2] http://fra.europa.eu/en/charterpedia/article/52-scope-and-interpretation-rights-and-principles EU Charter of Fundamental Rights, The European Union Agency for Fundamental Rights (FRA)

11. Young people, age 14-19 were asked in the 2010 study Privacy and Prejudice[3], conducted by The Royal Academy of Engineering (Paterson, L. and Grant, L. (eds) supported by three Research Councils, and Wellcome, about attitudes towards the use of electronic medical records, their concerns and questions centred on privacy, and data getting into 'the wrong hands'.

12. Trust in use of their confidential health data was affected by understanding data security, anonymisation, having autonomy and control, knowing who will have access, maintaining records accuracy, how will people be kept informed of changes, who will maintain and regulate the database, and how people will be protected from prejudice and discrimination [through use of their data].

13. The report concluded: *"These questions and concerns must be addressed by policy makers, regulators, developers and engineers before progressing with the design, development and implementation of EPR record keeping systems and the linking of any databases."(p40)*

14. On a small scale, we asked similar questions of young people on use of their education data. We include those findings later.

15. The Royal Statistical Society Data-Trust-Deficit with Lessons for Policymakers, 2014[4] measured public trust levels and found that individuals' trust in government to use personal data in their best interest is low. Only 11% of those asked in the 2014 surveys had a high level of trust in government to use their personal data in their best interest.

16. If public trust is to be increased, the use of personal data needs to return data sovereignty to individuals, and reduce data used for covert surveillance. Baroness Kidron talked in the House of Lords in January 2014 (Hansard), of creating a regulatory framework that protects young people from routine collection of their data, from it being stored and sold in perpetuity without recourse.

17. We see opportunity to address these issues in upcoming legislative changes, and to make the spectrum of public data work well, in a consensual and trusted relationship between individual and State, by restoring the rights of the individuals from whom data come to the core of data policy, setting public benefit as the central purpose of use, framed in good data security practices, data integrity, and other uses filtered in an ethics-based framework of decision-making.

Introduction - "There is a risk that their personal data may be collected or transferred without them being aware."

18. The 2014 report to which the consultation makes reference, *Children's online behaviour: issues of risk and trust - Qualitative research findings*[5], groups some known risks into a hierarchy, of 'contact' risks (e.g., unsolicited approaches from strangers), and 'conduct' risks (e.g., engaging in cyber-bullying). And it said, "*There is less consideration of content-associated risks (e.g. viewing inappropriate content), or the perceived repercussions of these risks*."

19. Risks children face now, include those they cannot perceive because they are hidden from the user. They can be disempowered through the mining of their individual personal data in machine-based decision making, in profiling, use of predictive data, and targeted behavioural influence, whether by commercial companies or under the care of the State.

20. Protecting children's integrity of their identity, their being online or offline, should be seen as sharing a common goal: enabling the development of their full potential and safeguarding children's future selves so as to protect them from harm generated as a child, following them in perpetuity. As Frankie Boyle wrote in the Guardian in 2015[6] whether of children or adults, *"Perhaps we've got so involved in the false selves we project on social media that we've forgotten that our real selves, our private selves, are different, are worth saving."*

21. Writing about the Investigatory Powers Bill, that will enable every person in the UK's web browsing history to be stored and used by third parties, he could also have been writing about the statutory guidance that makes web monitoring of children compulsory from September 5th 2016. He reminds readers that we need to consider what our internet history is. *"The legislation seems to view it as a list of actions, but it's not. It's a document that shows what we're thinking about."* Children think and act in ways that they may not as an adult. People also think and act differently in private from they

---

[3] Paterson, L. and Grant, L. The Royal Academy of Engineering (2010), Privacy and Prejudice: Young people's views on Electronic Patient Records. http://jenpersson.com/wp-content/uploads/2016/08/Privacy_and_Prejudice.pdf

[4] Royal Statistical Society Data Trust Deficit with Lessons for Policy Makers (2014) https://www.statslife.org.uk/news/1672-new-rss-research-finds-data-trust-deficit-with-lessons-for-policymakers

[5] Ofcom Children's online behaviour: issues of risk and trust Qualitative research findings (2014) http://stakeholders.ofcom.org.uk/binaries/research/research-publications/childrens/report.pdf

[6] The snooper's charter: one misspelled Google search for 'bong-making' and you'll be in an orange jumpsuit: Frankie Boyle (Nov 2015) https://www.theguardian.com/commentisfree/2015/nov/10/frankie-boyle-theresa-may-internet-surveillance

may in public. So the fact that our private online activity may become visible to the State, future employers or academic institutions — whether as photographs capturing momentary actions, or trails of transitive thinking via our web history — and those third-parties may make judgements and reach conclusions about us, correctly or not, behind the scenes without transparency, oversight or recourse, is of concern.

22. Children's personal data, which are now available from birth in health and may be joined to education data available from age 2, means that longitudinal data increasingly offers a richness and depth of life stories that has not been available before. For academic researchers this presents an opportunity to see into lives, and infer connections, and patterns that they could not otherwise. The same is true for other data users. This knowledge creates a power imbalance between what is known to the data user and what is known by the subject themselves. Power has the potential to be used for good, or not.

23. Data Protection needs reframed in many discussions as not about protecting data, although data security plays a big role in the discussion, but the purpose of protecting data is to protect the person from whom the data comes, from potential harm through abuse of power; labelling, stigma and discrimination, or any kind of unwanted intervention as a result of the knowledge obtained from their data.

24. The term 'datasharing' is often used when in fact copying and using data without consent is a more accurate description from the data subject's point of view. This introduction goes some way as to be an explanation why protecting children's data entrusted to schools — the personal data provided by parents and pupils themselves, combined with the individual attainment, behavioural and opinion based data created in schools — really matters. Who has access to these data and what they are permitted to do with it may affect our children in their everyday life, beyond school, and forever.

25. Risk for this generation through the covert manipulation of free will and behaviours online or censorship of their Internet access go beyond their own personal risk but have potential offline risk for the functioning of a fair and democratic society as we know it: influencing voting, emotional contagion (see the Facebook experiment), manipulated Internet search returns — to show only certain providers' services, goods, information about certain people, candidates or events.

I. Secondary uses of children's data collected aged 2-19

26. All the named data collected starting from the Early Years settings for children aged 2-19 at the time of collection, are processed to the National Pupil Database (NPD) and given away to third parties by the Department for Education (DfE). The NPD is one of the richest education datasets in the world and holds a wide range of information, extracted since 2000. Any school pupil's full educational record is made up of personal data given to schools by parents, and the pupil data created in school from testing and tracking; attainment records, absence, exclusions, sensitive data like ethnicity and date of birth, SEN, indicators of armed forces, and indicators of children in care.[7] It includes a number of different linked data collections from schools, Local Authorities and awarding bodies, processed by the DfE's Education Data Division (NPD User Guide, 2015, p5)[8]. We obtained the size of the database through Freedom-of-Information[9] as this is not published. 'The total number of Unique Pupil Numbers (UPNs) in the NPD as at 28/12/2015 was 19,807,973. This covers pupil records since 2000.'

A. Data releases from the Department

27. The National Pupil Database data are released outside the Department for Education process for academic research purposes. Those deidentified uses are not the subject of this submission. All the releases we mention here are those made by the Department of identifiable data. In addition to requests for use in public interest research from academic institutions, data have been released to commercial companies, charities and journalists. Recipients of sensitive identifying individual-level personal data include national papers[10] and television[11]. An August 2016 FOI request shows not all releases are publicly documented. Since 2012 children's data were given to the Home Office 18 times, and the Police made 31 requests.[12]

---

[7] *DfE Common basic data set (CBDS): database https://www.gov.uk/government/publications/common-basic-data-set-cbds-database*

[8] *Copy of the 2015 NPD user guide http://defenddigitalme.com/wp-content/uploads/2016/08/NPD_user_guide.pdf*

[9] *FOI request for total pupil numbers in the NPD https://www.whatdotheyknow.com/request/pupil_data_national_pupil_databa_2*

[10] *FOI request September 2015 https://www.whatdotheyknow.com/request/293030/response/723407/attach/5/The%20Times.pdf WhatDoTheyKnow.com*

[11] *https://www.whatdotheyknow.com/request/293030/response/723407/attach/10/BBC%20Newsnight.pdf*

[12] *FOI request July 2016, Pippa King https://www.whatdotheyknow.com/request/pupil_data_sharing_with_the_poli WhatDoTheyKnow.com*

28. The DfE publishes online a spreadsheet register[13] of third-party recipients to whom it has released data since 2012 through its own application and approvals process (DMAP). Of the registered 462 releases of identifiable data that went through the DMAP in 2012-2014, 53 were aggregated data. All others are individual level. A recent May 2016 update shows 650+ releases (2012- 2015).

B. Privacy notices and legal uses

Question 5 in the consultation asks what roles schools can play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

29. Schools use a variety of system providers to collect a vast amount of personal data from pupils, and create additional data in schools about children's educational achievement, behaviour, attendance, absence and more. Schools are ineffectively informed about national use of their pupils' data collected locally. Communication is on transmit mode only from the national Department, made through an overly complex and under transparent template privacy notice, which leaves a knowledge gap between the Department and schools. It is potentially big enough to protect the Department from legal challenge on use of pupils personal data, but not to rescind its responsibility to do the right thing. The Department is accountable to make sure the public expectations are met that our data are safe and used transparently with 'no surprises' (Wellcome, 2015)[14], the alternative, keeping things hidden was to the cost of public trust in use of health data in the care.data programme and has ongoing repercussions for public interest research, and individuals' accessing healthcare.

30. Changes in 2012-13 Education policy and law, permitted the release of individual data, by amending section 114 of the Education Act 2005, section 537A of the Education Act 1996, and together with the 2009 Prescribed Persons Act changed the purposes for which data about individuals could be released, and changed to whom it could be given. When the database was first opened up, then Ministers gave verbal assurances the Department was not interested in names.

31. The uses that were limited in 2003, to a "*small number of technical staff engaged in collating the pupil level data and creating the profiles have access to pupils' UPNs and names. Analysts in the Department and partner agencies (Ofsted, QCA and LSC) have access to anonymised profiles for use for statistical purposes only*.[15]" as described by Stephen Twigg, are long since exceeded.

32. For detail of the legislative changes before 2007 see *Children's Databases - Safety and Privacy* (Anderson, R., et al. 2006 pp112-115) [16]. The 2012-13 changes enabled individual pupil information to be released for the first time:

> *"Persons who, for the purpose of promoting the education or well-being of children in England are— (i) conducting research or analysis, (ii) producing statistics, or (iii) providing information, advice or guidance, and who require individual pupil information for that purpose."*

33. The revised privacy notice template of May 2016, included for the first time, a link to the organisations that the DfE gives individuals' data, including commercial companies, charities and journalists, recipients of children's identifiable personal data from the National Pupil Database between 2012 and December 2015.

34. Notices adapted from the national template and then used in schools are however widely variable in how they reach schools, via Local Authorities or other channels depending on the school structure, and those forms content we have seen vary from including as little as one line on purposes, 'Data may be shared with the Department for Education'.

35. However even if children in school between 2000 and 2012 had read the then school issued privacy notice in detail and knew that their data from the census was sent to the Department for Education, then passed on to organisational bodies in the style of Ofsted or HESA, no child whose data were collected before 2012 has been contacted to tell them that the law changed in 2012-13 to permit the giving away of their named, confidential personal data, or of giving out individual level data to journalists, charities, and commercial business.

36. Further the Department appears to have had no clearly recorded legal basis for handing out sensitive data.[17]

---

[13] NPD third party online release register https://www.gov.uk/government/publications/national-pupil-database-requests-received

[14] Wellcome Trust Briefing (2015) Ensuring the effective use of patient data https://wellcome.ac.uk/sites/default/files/ensuring-the-effective-use-of-patient-data-briefing-aug15.pdf

[15] Hansard 14 Apr 2003 : Column 557W—continued http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030414/text/30414w22.htm

[16] Children's Databases - Safety and Privacy (Anderson, R., et al. 2006) http://www.fipr.org/childrens_databases.pdf

[17] https://www.whatdotheyknow.com/request/pupil_data_sensitive_data_releas#comment-69968

37. These gaps needs attention if the uses of the pupil data are to meet current and future legislative requirements, particularly with regards the EUGDPR on consent, limitation of purposes, profiling, necessity, and proportionality.

38. At the time of writing the School Census and Early Years Census collection are about to be further expanded, beginning in the 2016-17 school year[18]. The collection has had no privacy impact assessment[19], no public or parliamentary debate.

39. Given recent Supreme Court ruling on the limitation of purposes, no provision for removal of information at third parties contravening Google Spain[20], and interference with privacy, it should be examined as to its legislative basis.[21] The purpose of the collection for country-of-birth and nationality at national level are not being well communicated to pupils, or schools.[22] While 'no requirement' is made to see passports, *"The country of birth would be expected to appear on — or be derived from — the child's birth certificate or passport."* Wording that leads some schools to ask for passports.[23]

40. The DfE school census video[24] made for school staff, explicitly says schools staff need not get consent, because there is a statutory gateway for the collection, and schools cannot be held accountable for breach of pupil confidentiality — so the Department for Education takes that decision and responsibility away from schools although the Minister has said, *"We do not advise schools directly on their collection and processing of personal data or regulate their compliance with the Data Protection Act."*

41. The same video does not tell them about any expanded purposes of the data use since 2012 changes. They indirectly therefore tell schools to rely therefore on fair processing but don't inform them explicitly, simply and transparently about all the Department releases of data to all third parties, so schools can't fair process because they aren't given simply all the facts to share.

42. Privacy notices policy at the Department for Education fails to adequately inform children of uses of their data, fail to take responsibility for communication if they can be amended at will after the data collection, and fail to offer the opportunity to remove or correct the data subjects's data before the purposes and users are amended.

43. We were told that the Director General for Regulation at the UK Statistics Authority wrote to the Department for Education calling for improved transparency and handling in April.[25] Much remains to be done to achieve this. See our FAQs for more information: http://defenddigitalme.com/faqs/ and sample case studies of use.

C. Subject Access Request rights — are data accurate and if not how do I correct it?

44. The Information Commissioner's Office has made it clear to the Department that in principle it supports data subject good practice rights of access[26] to enable individuals to check that the data held in a database are accurate and correct them if necessary. Given that these data are used for direct interventions it is vital data are accurate. The effect of an incorrect address being used by academic researchers for a health or education survey is potentially quite different from it being used by the Home Office. The Department refuses subject access requests, basing withholding on exemption Section 33 in the Data Protection Act. This exemption is used where data are held for research purposes, where data are not used to have any direct effect or intervention with individuals. Our case studies show that named interventions[27] use these data, as well as being used by at least one Data Processor to create predictive scoring on children, which is fed back to Local Authorities and schools. These data are processed without the knowledge or consent of parents or pupils. At present national newspaper journalists have greater access to children's identifiable data in the NPD than parents or children themselves. Clearly any changes in this would need strict regulation to enable appropriate and approved access.

---

[18] *http://blogs.lse.ac.uk/parenting4digitalfuture/2016/07/19/school-census-changes-add-concerns-to-the-richest-education-database-in-the-world/*

[19] *http://defenddigitalme.com/wp-content/uploads/2016/08/Gibb_response_Aug2016_36177.pdf*

[20] *http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf Google Spain ruling*

[21] *http://panopticonblog.com/2016/08/25/donald-wheres-schedule-3-condition-share-information-aboot-troosers/*

[22] *https://www.buzzfeed.com/laurasilver/parents-are-worried-about-schools-plan-to-ask-what-country-t?utm_term=.mmolpAkP#.de9P4yJX*

[23] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544214/2016_to_2017_School_Census_Guide_V1_2.pdf*

[24] *https://registration.livegroup.co.uk/efa/contenttabs/embed.aspx?dfid=12620&ctid=242&cat=1937 (listen from 40 seconds in)*

[25] *http://defenddigitalme.com/2016/04/director-general-for-regulation-uk-statistics-authority-suppports-call-for-transparency-and-better-data-handling-of-20-million-pupils-data/*

[26] *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/*

[27] *http://defenddigitalme.com/wp-content/uploads/2016/04/DDM_shared_examples_April2016.pdf*

D. Public Awareness and Attitudes towards the National Pupil Database

45. We set out to make a preliminary qualitative assessment of awareness in school staff, parents and young people about the NPD, asking them what they know about how children's data collected in school and its use beyond state education. These results could be seen as a pilot for a broader engagement in how the public relate to information and NPD data, and its use.

Summary of responses gathered

46. In autumn 2015, we asked school staff about when they last received or made an update to their own privacy policies, but we encountered consistent difficulty asking about it, as none were familiar with the concept or uses from the NPD. In this atmosphere we promised anonymity to schools and staff in the publication of their responses. Students who gave us recorded interviews gave us only their first name, age, and hometown. We did not ask for contact details to re-contact. We focussed on questions of awareness of data existence and use, and asked young people about control of their data.

Schools - talking about their pupil data

47. From a list available online of all state sector schools, and 100 asked, we had replies from 30 primary and 45 secondary schools in Dorset, East and West Sussex, in London, Oxfordshire, and Yorkshire. We selected a spread between rural and city schools, those under Local Authority or academies. We did not ask Free Schools. When we first asked schools about it by email or telephone, respondents said it was because they had never heard of the NPD and felt unable to give an informed opinion. We then instead asked for concrete copies of privacy notice documents via FOI and comment. Privacy policies returned demonstrated a wide variety of wording and consistent gap in communicating NPD use.

Education practitioners questions and answers

48. We interviewed 100 teaching or affiliated school staff face-to-face at three education events in spring 2016. None were aware of the NPD. Most were aware of the school census but did not know who see pupil data outside school or the Local Authority. Some suggested only statistics are shared outside their school or at national level. Ten staff sampled from Independent schools asked at the Festival of Education, in June, were also unaware of data uses though one had heard of the database created from the census, as they used a copy of personal data collected for alumni fundraising.

Parents questions and summary answers

49. We interviewed 100+ parents face-to-face in November 2015 at the Mumsnet Blogfest in King's Place, NW London. These were parents of children, in education in England, 90% in state education. We discounted 2 home schooling. They came from across England. No one had heard of the NPD or knew that named identifiable data are released beyond school for use by third parties. All were surprised that commercial businesses and journalists could access data. Comments ranged from questions of trust, to a lack of concern 'as long as they've not done anything wrong with it.'

Young people questions and their answers

50. We gathered interviews over two separate hours on two days in May 2016 at the University of Sussex with 25 individuals under 35, only if they had been to school in England, and in different parts of the country. Six agreed to recorded statements. We introduced the idea of the NPD. None had heard of it. We explained that the data has been opened up to third parties since 2012, the approvals process, rules for use, and the wording of the legislation on uses. Comments from interviews include:

51. Ben 26, from Reading: *"I don't think commercial businesses should have access to student data. You have not necessarily been exploited, but definitely used."*

52. Catherine, 21, from Gloucestershire: *"Parents and pupils should have access to their own data and should know who else has it. I don't think anyone else should have access to the identifiable data without consent."*

53. Johann 18, from Paris (completed A-levels in England): *"I'm not surprised my data is used by others, probably some of it is used for good causes, but we should know who has it […] we should define our privacy (not the government) and they should ask us before they use it for anything we don't expect."*

54. John 30, from UK: *"I've never heard of the National Pupil Database. I'm really surprised, it's a bit weird. I don't think anyone should have it unless it's to do with my education. We should definitely be asked."*

55. Ruby 28, from Newcastle: *"I'm surprised to hear my school data could be used outside schools without my consent. It's a personal thing and can affect lives."*

56. Steph 19, from London: *"In school I remember being told to do biometric fingerprints for buying lunch. We had no idea what it would be used for and I've no idea if they ever delete them. Parents should be asked for consent.As pupils get older we should decide ourselves."*

57. Public and school professionals' familiarity with the National Pupil Database is almost zero. If uses across the data spectrum are to best serve our public interest needs, then consistent legal, safe and transparent policy and practices are needed across education, underpinned by accountability. Respect for the opinion and rights of children (many now in the NPD) about how their data can and should be used must be restored, as the foundation of all data use is public trust.

II. Surveillance of children's use of the Internet

58. Without Parliamentary debate or public discussion, children's internet use will be monitored by third parties from September 5th 2016, under statutory guidance issued by the Department for Education. This is despite widespread associated concerns – including choking off free speech, religious freedom, and staff feeling vulnerable — shared with the Joint Select Committee for Human Rights by experts in education and security legislation.[28]

59. The brief paragraph 75 in The Department for Education (DfE) "New measures to keep children safe online at school and at home"[29] statutory guidance, *Safeguarding in Schools*, will impose a change from a duty 'to consider' web monitoring to one that 'should ensure' it for educational establishments, excluding 16-19 academies and free schools.

60. We suggest that this proposal which will monitor every child in England's in-school's online activity and communications is significant and opens a slippery can of worms[30]. Some providers manage the monitoring entirely offsite outside school, removing the oversight of the classroom teacher from the process. It is unclear whether Bring-Your-Own-Device policies offered by some well known providers in the market means surveillance software is carried into personal time and use at home, yet there has been no standard code-of-practice to tell schools this would be unacceptable practice, to accompany the guidance.

61. Before imposing this statutory practice, its cost, technical risks and impact where it has already been used in practice, should be assessed more deeply and widely debated in public and Parliament. Due diligence of providers should ensure appropriate standards and regulation when providers may have access to millions of children's computers and devices and it is left to independent experts to demonstrate flaws that put children at risk[31]. Basic flaws such as using a default password of "password" to connect clients to its servers should never happen.[32] This programme has been imposed without understanding its impact or checking that known issues or questions asked in consultation[33] have been solved.

62. Children aged nine and under were among 3,955 people reported to Channel in 2015, up from 1,681 in 2014.[34] How many of these stemmed from being flagged by algorithms, or web browsing and monitoring?

63. Children have rights to be able to access information. Web monitoring, the surveillance of search terms and web uses, looking for keywords and logging behaviour is not to be confused with web filtering, which restricts access to certain material to protect children from content deemed inappropriate. Others feel it is ineffective[35] and counter productive, and lack of communication and transparency about its implementation even leaving parents feeling betrayed.[36]

64. A statutory requirement should be explicit in its terms. Yet what "has appropriate filters and monitoring systems in place" means for different age groups, types of pupils, staff, school and home settings, is not.

65. On filtering however there are also concerns about how framing can mean over cautious implementation restricts children's rights to information. The UN Special Rapporteur's 2014 report on children's rights and freedom of expression

---

[28] http://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/legislative-scrutiny/parliament-2015/extremism-bill/?type=Oral#pnlPublicationFilter

[29] https://www.gov.uk/government/news/new-measures-to-keep-children-safe-online-at-school-and-at-home

[30] http://schoolsweek.co.uk/mandatory-web-monitoring-in-schools-opens-a-slippery-can-of-worms/

[31] July 2015, Security flaw found in school internet monitoring software https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software

[32] https://www.techdirt.com/articles/20150715/10274131649/shocking-software-used-to-monitor-uk-students-against-radicalization-found-to-be-exploitable.shtml

[33] http://defenddigitalme.com/wp-content/uploads/2016/04/DfE_consultation_Feb2016v4.pdf Keeping Children Safe in Education consultation response

[34] http://www.npcc.police.uk/Publication/NPCC%20FOI/CT/02616ChannelReferrals.pdf

[35] http://www.wired.co.uk/article/schools-monitor-children-internet-use

[36] https://webdevlaw.uk/2015/10/30/the-ugly-truth-behind-uk-schools-monitoring-students-keyword-searches/

stated: "*The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risks*."

66. This new guidance, '*Safeguarding in Schools'* makes no attempt to ensure informed changes about new national policy on web monitoring reaches children and parents. The potential for risk undermining trust between teacher and pupil should not be underestimated. The chilling effects associated with online surveillance[37] and long term effects and impact on children's curiosity, willingness to take risk, innovate, and challenge thinking of the day, are as yet unassessed.

A. Biometrics and surveillance of children in schools online and through new technology

67. The opportunity for online surveillance of children through new web applications has been lauded by some. Nicky Morgan former Education Secretary at the BETT trade show in both 2015 [38] and 2016[39], praised an app that enabled parents, or others, to track children's movement.

68. The general use of apps in schools, their educational value and technical safety, appears unregulated and without oversight. We have started to look at privacy policies in some commonly used apps, and in particular those who send enrolled children's personal data abroad, typically to the US. Many aware parents agree with academics who feel we are sleepwalking into the use of these systems which pose risk.[40] Some commercial companies have been to date unresponsive to questions on their practices and children's privacy rights.

69. Schools can fail to ask parental permission for signing up children in the classroom and inadequate attention is given to privacy or long-term implications. We have begun conversations to see whether opportunity to improve teachers' understanding of Data Protection and privacy in the classroom can come through teacher training — up to date with current technology, and with privacy rights. If and how the current teaching training curriculum includes this in a consistent and up-to-date way we don't yet know, but if not, it is a serious gap that needs filled.

70. The first instance of a school in the UK using RFID technology to track individual children's activity and behaviour in schools was scrapped in February 2013 at West Cheshire College after significant financial cost.[41]

71. The full national extent of using fingerprint and other biometric technology in schools is unknown.[42] Since 2001 iris scanning and facial recognition have also been used in schools.[43] There is no transparent assessment of the technological capacity, false positives, cost and benefit, or effectiveness. There is no clear oversight of technologies specific to schools.

72. These practices seem to be praised before they are proven to be of benefit, or before measuring their impact against a business plan and cost, or indeed as technology becomes increasingly invasive, against ethical standards and human rights legislation, or even it appears often, before communication to parents and pupils of its use.[44]

73. The report in the consultation mentions awareness of access to inappropriate material but does not mention access to material which is targeted at them with the intent of behavioural change. Some apps in school are explicit in their intent to change behaviour. Others have indirect or covert influence, and nudge behaviour. How these behaviour changes and their indirect effects will effect children's willingness to search freely for information or concern about what being watched online may mean appears to have little research to date. Very recent preliminary studies indicate that 18-24 year olds, the youngest age group asked in a survey[45], were the least likely to trust biometrics. Questions remain if schools using theses technologies are gambling with children's identities.[46]

---

[37] *Penney, Jon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, 2016. Available at SSRN: http://ssrn.com/abstract=2769645*

[38] *https://www.gov.uk/government/speeches/nicky-morgan-speaks-at-the-2015-bett-show*

[39] *https://www.gov.uk/government/speeches/nicky-morgan-bett-show-2016*

[40] *https://www.theguardian.com/education/2016/mar/05/education-parent-children-behaviour-app*

[41] *https://www.whatdotheyknow.com/request/procurement_procedure_regarding#incoming-446369*

[42] *https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf*

[43] *https://www.youtube.com/watch?v=acbSj5m5o5g*

[44] *https://rfidinschools.files.wordpress.com/2013/10/west-cheshire-college-10th-december-2012-foir-fs50488835-report.pdf*

[45] *http://cyber.uk/biometrics/*

[46] *And therein lies another issue: with the potential for life-long consequences, are pupils, some below the age of 16, competent to opt in to such a scheme?*

Conclusion

74. For children in educational settings, the people responsible for systems, policy and practice can compromise children's privacy rights and civil liberties, not only for their school life but potentially for their whole lifetime, when they collect personal and other data without consent or communicating an effective understanding of what is being signed up to.

75. The Joint Committee on Human Rights previously found, "*failure to root human rights in the mainstream of departmental decision-making*."[47] Children's human rights are failed by current practice in the use of personal data entrusted to the State and released onwards to third parties.We suggest careful consideration by the Committee to the upcoming legislation and amendment to address an appropriate balance in this area, especially with regard to children, their personal data used for public benefit, for commercial profit, and uses to their potential personal detriment.

76. Consistent safe data policies, settings in which data are accessed, standards and oversight — how public data not only 'can be' used, but 'should be' used, accommodating consensual data subject rights — are needed across public data, to make data secure, future-proof public trust, and above all to ensure our young people feel sovereignty of their personal data is returned to them, so that they no longer feel, they have "*not necessarily been exploited, but definitely used."*

77. The quantity of apps and online tools is increasing and being actively encouraged by those who profit from a growing ed tech market[48] and many are exciting with opportunities to learn, create, collaborate and have fun. The front door to our children's data "for government, educators, companies and investors" is wide open. Tools for schools to use to assess whether the latest digital offering is legal, and educationally and ethically sound however, seem to be lacking.

78. Web monitoring and filtering using third party providers is exposing children to new security risks.The loose definitions of inappropriate content used setting Internet filters, can prevent children from gaining access to information that can support them to make informed choices, and may exacerbate rather than diminish children's vulnerability to risks.

79. The CMA report (June 2015)[49] on consumer data, highlighted that to secure the benefits of data, people should know when and how their data is being collected and used and decide if and how to participate.

80. The House of Commons Science and Technology Committee 2014 in their report, Responsible Use of Data[50], said the Government has a clear responsibility to explain to the public how personal data is being used. This needs to be actioned by government. Their Big Data Dilemma 2015-16 report, concluded:

> "*seeking to balance the potential benefits of processing data (some collected many years before and no longer with a clear consent trail) and people's justified privacy concerns will not be straightforward. It is unsatisfactory, however, for the matter to be left unaddressed by Government and without a clear public-policy position set out. The Government should clarify its interpretation of the EU Regulation on the re-use and de anonymisation of personal data, and after consultation introduce changes to the 1998 Act as soon as possible to strike a transparent and appropriate balance between those benefits and privacy concerns."*[51]

81. We conclude that there is not only a risk but already a widespread reality that children's personal data are collected and transferred without them being aware of it. There is also concern that the online activity of children is being used by third parties to make decisions about them without transparency of how those decisions were reached or to assess their impact.

82. Action is needed to safeguard children from use of their data gathered by the State or commercial companies in the course of their education and without transparency, or clear oversight, for a range of secondary purposes which can expose them to risk from outside third parties, decisions based on inaccurate data, or misinformed intervention without clear course of redress. Upcoming legislation may offer opportunity to create Baroness Kidron's suggested framework that protects young people from routine collection of their data, from it being used in perpetuity without recourse.

August 26, 2016

---

[47] *Joint Committee on Human Rights Data Protection and Human Rights Fourteenth Report of Session 2007–08 http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf*

[48] *The front door to our children's personal data in schools - Jen Persson, February 2016 http://jenpersson.com/front-door-childrens-data-for-government-educators-companies-investors-britain-globally/*

[49] *CMA report (2015) Commercial use of consumer data https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf*

[50] *The House of Commons Science and Technology Committee 2014 Report, Responsible Use of Data http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf*

[51] *The Science and Technology Committee Big Data Dilemma Report (2015-16) http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf*