Further Education and Research Bill: House of Lords 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. More information: http://defenddigitalme.com/ 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

Summary of implied changes in Part 3 of the Bill - Duty to Provide Information[1]

1. The bill[2] amends Section 54 of the Further and Higher Education Act 1992 (duty to provide information)[3] which includes "*such information relating to the provision which has been made by a local education authority* ***in respect of any pupil*** *at an institution as the authority may require for the purposes of claiming any amount in respect of the pupil from another authority under [F5regulations under section 492 or 493 of the Education Act 1996] shall, where the institution becomes an institution within the further education sector, be provided to the authority by the governing body of the institution*."

2. Local use is replaced with national use. Vague definitions and open wording mean that in effect any obvious previous local limitations of who will receive the data is removed: individual pupils' data must be given to the Secretary of State.

3. The purposes in old legislation (Section 54 of the Further and Higher Education Act 1992) are changed from what "the authority may require for the purposes of claiming any amount in respect of the pupil from another authority" to it appears limitless boundaries on the purposes for which the Secretary of State may use the data as long as generically to do with FE: "as the Secretary of State may require for purposes connected with further education" .

4. Amendments are needed to Part 3 to ensure that the intent of the Bill to provide copies of individuals personal confidential data for the purposes of the Secretary of State is deliverable without putting young people's privacy and public trust at risk today, or in the future. Children's data becomes adults' data, and builds a population-wide database over time. In framing safeguards it may be helpful to think not as student data, but for what purposes or organisation and with what oversight committee members would like their own personal data used.

Meeting existing Data Protection legislation, Human Rights law and other upcoming legislation

5. Data protection Act 1998 and Principles 1-8: Requirement to hold adequate but not excessive personal data: (Principles 3 and 4)[4] How will any new collection be aligned with the Principles of the Data Protection Act 1998?

6. Data accuracy: Principle 4 "Personal data shall be accurate and, where necessary, kept up to date."[5]. This is supported by data subject good practice rights of access[6] to enable individuals to check that the data held in a database are accurate and correct them if necessary. How will this be upheld in the SoS new national database?

7. Retention and deletion: How frequently will data be transferred to national level? Will the Secretary of State be able to keep and use it forever?

8. Limitation of purposes: The July Supreme Court ruling on the limitation of purposes, no provision for removal of information at third parties contravening Google Spain[7], and interference with privacy, should be examined with respect to the new plans for gathering data and as to its legislative basis on consent and right to revoke consent.[8]

---

[1] http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0082/cbill_2016-20170082_en_1.htm

[2] http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0082/cbill_2016-20170082_en_3.htm#pt3-l1g38

[3] http://www.legislation.gov.uk/ukpga/1992/13/section/54

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

[5] ibid

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

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

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

9. Upcoming Data Protection legislation (GDPR) already in place and enforceable from May 25, 2018 requires additional attention to fair processing, consent, the right to revoke it, to access one's own and seek redress for inaccurate data. Where FE students may start courses at sixteen, many applicants are fifteen. "The term "child" is not defined by the GDPR. Controllers should therefore be prepared to address these requirements in notices directed at teenagers and young adults."[9]

10. The Rights of the Child: Data policy and practice about children's confidential data will 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 if these data will be used without consent. Similar rights that are included in the common law of confidentiality

11. 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.

12. 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 legally and fairly process personal data before transferring it between themselves.[10] How will fairness be addressed if students cannot be told the purposes for their data extraction for generic uses "as the Secretary of State may require for purposes connected with further education."

13. The EU Charter of Fundamental Rights[11], 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.

14. The forthcoming Digital Economy Bill 2016 will still further expand who may have access to all those confidential datasets across government and public bodies, and for what purposes individuals' personal data may be used, and the draft bill includes provision for Student Loans providers access to student data, and on Debt recovery, to single out just two.

15. Opening Further Education pupils' data for extraction by the Secretary of State and use across Government [by dint of the Digital Economy Bill] will enable access to a more joined-up dataset, a lifetime of personal confidential identifiable data from 2 years of age into work after Further Education, including datasets in HMRC, DWP, and The UK Department for Business, Energy & Industrial Strategy (BEIS)[12], from millions of individuals in perpetuity. Data it appears will never be deleted, and may be used indefinitely or see its scope changed, without any sunset clause.

Suggested areas for amendments or required guidance

16. Purpose and scope change limitations: Safeguards and oversight are needed for consent and the rights of FE students to object to uses which change the nature of the use from the purpose which they gave consent to its use or it was collected.

17. Transparency register: There should be a transparency register to show all releases from the dataset similar to the current transparency tool at the Department for Education, the spreadsheet register[13] of third-party recipients to whom it has released data since 2012 through its own application and approvals process which works as long as a commitment to transparency is upheld. However the DfE has not included Back Office uses, shown in August 2016 through FOI to include undocumented releases of identifiable data, to the Cabinet Office, Home Office, and Police since 2012.[14]

18. Subject Access Requests: Providing the public ways to access copies of their own data (Subject Access Request) and the publication of Transparency Registers or personal reports to list all releases of data (showing how data have been used) can also demonstrate the public benefit intended from that use and foster trust. As an example, academic public interest application for data uses in safe settings are published by the Administrative Data Research Network (ADRN)[15] the current UCAS research third party. Uses of the Government copy of any new Further education students' database would by contrast be used without oversight and carried out in secret.

19. Consent procedures should be strengthened for collection since The Secretary of State will become the Data Controller. For example to compare, HE applicants can't opt out on collection of UCAS sharing their data during admissions purposes, for regulatory or statutory purposes, or for public interest academic research (currently explicitly and only with the

---

[9] http://www.twobirds.com/~/media/pdfs/gdpr-pdfs/24--guide-to-the-gdpr--children.pdf?la=en

[10] 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

[11] 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)

[12] Nick Boles MP, Jan 25th 2016, at the Education Select Committee

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

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

[15] https://adrn.ac.uk/research-projects/approved-projects/

ADRN): *"We also share personal information from your application with University of Essex for use through the Administrative Data Research Network (ADRN), including linking to other data sets, for as long as is necessary to enable research about higher education, where there is a potential public benefit. Data is only made available for approved non-commercial research projects. Your data is only made available through the secure access provided by the ADRN and researchers can only access your data once your identifying details, such as name and date of birth are removed."* [16]

20. In HE today for example there is a nuanced consent process for other third party purposes which must be respected by all uses of the data after collection. HE Applicants have the option to consent separately from data use for other purposes:[17]

    - With universities and colleges if students are unplaced
    - With the Student Loans Company
    - With third parties such as banks and insurance companies
    - Additionally, applicants can opt to receive targeted mailings or products from UCAS Media Ltd on behalf of selected companies and organisations offering services to students. UCAS do not share applicants' personal data with these organisations.
    - Applicants opting to receive these mailings can choose separately whether to receive information about careers, education and health issues as distinct from commercial marketing information.
    - Applicants can also opt out of receiving information at any time.

21. Without clear purposes processing cannot be fair or consent informed If the SoS held copy of the database is going to be used for anything of the above, such as with the Student Loans Company (see the Digital Economy Bill), then applicants must understand this when data are collected and consent choices must be respected. The Secretary of the State and any approved parties must respect these uses but "the Secretary of State may require for purposes connected with further education" is so open as to be meaningless. Is applicant data from children to be used by any public body or third party to find interesting things, interesting group characteristics, or interesting individual characters[18] at future political whim?

22. Ability to withdraw consent: Required in the GDPR. Again as a comparison, UCAS respects the Data Protection Act 1998 and caters to the upcoming EUGDPR legislation (Article 7(3) of the GDPR which gives data subjects the right to withdraw consent at any time and requires "*it shall be as easy to withdraw consent as to give it*." How will the State enable the right to prevent sharing with the very bodies which students have already said no in the original provision to UCAS and how will scope creep prevent the unfettered expansion of these uses in future.

23. Clarification of the legislative purpose of use by the Secretary of State and its boundaries is needed. To avoid repeating similar legislative changes which have resulted in poor data practices using school pupil data in England age 2-19, we would like to ask the Committee to consider whether the intent of the Bill is to give out identifiable confidential data of young people, potentially under 18, for commercial use? Or to give journalists and charities access? For unfettered access by government departments and agencies without transparent oversight such as police and Home Office? These are today's uses by third-parties[19] of school children's identifiable and sensitive data from the National Pupil Database when similar changes were made in 2013 to give a copy of all pupils' data from schools to the Secretary of State for Education. The Secretary of State for Education deemed these appropriates uses in 2013 and amended the Education Act to enable use of children's confidential personal data without their consent in commercial products, papers[20] and TV journalists[21]

24. Review or sunset clause: We propose a forward review date or sunset clause built into the legislation for the use of data by the Secretary of State with respect to children's rights because technological change, for example in between the founding of the National Pupil Database and in the sixteen years since, 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.

---

[16] https://www.ucas.com/corporate/about-us/privacy-policies-and-declarations/ucas-declaration

[17] https://www.ucas.com/corporate/about-us/our-personal-data-policy

[18] https://www.whatdotheyknow.com/request/293030/response/723407/attach/5/The%20Times.pdf

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

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

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

Conclusion

25. The Joint Committee on Human Rights previously found, "*failure to root human rights in the mainstream of departmental decision-making*."[22] 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 avoid repeating this in FE students' data in this legislation.

26. Purposes need limitation in Part 3 of this Bill. The government-wide use of all public datasets is set out in the Digital Economy Bill 2016, will use more identifiable data for a wider range of purposes, together with increasing the use of data that have been linked with multiple datasets across different sources. This dataset will likely also be made available by dint of this Bill. Respondents to the Cabinet Office 2016 consultation, Better Use of Data in Government, "felt strongly that publicly-held data should not be accessed by researchers for commercial or profit-making purposes."[23]

27. A focus on affirmative consent is required to future proof trust in secondary use. The GDPR has particular provision for children and the right to an easy route to revoke consent at any time. GDPR Article 9 requires more – "explicit" consent – for the processing of "special categories of personal data." and not all uses are exempt under the 'research' exemptions. Judgment of the Court of Justice of the European Union (C-201/14)[24] (Oct 2015) reiterates this across public bodies.

28. People should know when and how their data is being collected and used and decide if and how to participate. The same spirit of the CMA report (June 2015)[25] on consumer data, highlighted that to secure the benefits of data, and applies here. Before use, this should be assured through consensual collection and fair processing. After processing the trustworthiness of the organisation using the data should be demonstrable through a transparency register.

29. The House of Commons Science and Technology Committee 2014 in their report, Responsible Use of Data[26], 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 […] strike a transparent and appropriate balance between those benefits and privacy concerns."*[27]

30. Consistent safe and transparent data policies, the settings in which data are accessed, their data use standards and oversight are needed across public data — how public data not only 'can be' used, but 'should be' used in line with data subject rights, to make data secure, future-proof public trust, and to ensure our young people feel autonomy of their personal data is returned to them, so as adults they no longer feel they have "*not necessarily been exploited, but definitely used."*[28]

31. Amendments to Part 3 and detail are needed to safeguard children from unexpected uses of their personal data gathered by any organisation in the course of their education and its use without transparency, or clear oversight, exposure to risk from third parties, decisions based on inaccurate data, or misinformed intervention without clear course of redress.

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

defenddigitalme
November 24, 2016

---

[22] 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

[23] http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0045/17045.pdf

[24] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf

[25] 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

[26] 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

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

[28] Public voice and pupil data, from our research paper, Data for Policy Conference 2016 http://defenddigitalme.com/wp-content/uploads/2016/09/58_Persson_PRINT_last.pdf