Online Learning as a Commons:

Supporting students' data protection preferences through a collaborative digital environment

by **Janis Wong, Lea Racine, Tristan Henderson, and Kirstie Ball ***

Abstract: The COVID-19 pandemic has accelerated the adoption of technology in education, where higher education institutions had to implement online teaching models overnight, without time for due consideration of appropriate data protection practices or impact assessments. The General Data Protection Regulation (GDPR) attempts to limit the negative effects caused by the digitisation of education such as lecture capture, tutorial recording, and education surveillance. The GDPR, however, may be insufficient in removing the power imbalance between students and their institutions, where students as data subjects have no choice but to accept their institutions' terms or be locked out of academia. To increase protection of students' autonomy, we propose an online learning data protection-focused data commons to support their agency with regards to protecting their personal data. We explain how a commons could apply to online learning, then develop and test an application to put the commons into practice. From our results, we find that although over 50% of students trust universities and staff with their online learning personal data, more transparency on institutional policies and data protection rights can support higher online learning participation rates, help mitigate potential data protection harms, and give students agency over their personal data beyond consent. We conclude that further research is required to move away from consent as the lawful basis for tutorial recordings, support inclusive online learning pedagogies, and balance the implementation of educational technologies with the need to deliver online learning to benefit students' academic experience.

Keywords: online learning, commons, data commons, data protection and education

Recommended citation: Janis Wong, Lea Racine, Tristan Henderson, and Kirstie Ball, Online Learning as a Commons: Supporting students' data protection preferences through a collaborative digital environment, 14 (2023) JIPITEC 251 para 1.

A. Introduction

1 Education has long been influenced by technology with students, staff, and institutions adopting new tools to enhance the academic experience, and more innovative and collaborative ways of learning. Due to the COVID-19 pandemic, the adoption of online learning technologies became mandatory as university campuses closed and education shifted from physical classrooms to digital ones. While tools such as lecture recordings and examination monitoring can help make education more accessible and equitable by enabling online teaching exams, they may also hamper students' learning experiences, particularly where they are not able to opt out of such practices. Further, there are questions as to whether these technologies are effective in enabling equitable access and desirable education outcomes. By adopting these technologies, more student personal data are being collected, stored, analysed, and shared. To ensure that these data are best protected, higher education institutions

("HEIs") have to follow data protection regulations such as the General Data Protection Regulation ("GDPR"),[1] and have data protection officers, fair use policies, and conduct a data protection impact assessment where appropriate. However, the power imbalance between students as data subjects and their institutions could weaken the data protection options available, particularly where not agreeing to the use of certain technologies can lead to being locked out of academic and career opportunities. As data collection of the teaching process in HEIs increases, it is important to provide data subjects with the option to improve their understanding of who, what, and how their personal data are being used and ways in which they can opt out. This includes helping them to understand their data protection rights and support them in exercising those rights without negatively affecting their ability to participate in online learning.

2 In this paper, we propose a socio-technical data protection-focused data commons for online learning to support students' agency in protecting their personal data. The commons aims to provide data subjects with the resources to improve their understanding of how their institution manages their data and what data protection rights they have. It also enables data subjects to have conversations with other students or experts about any questions or concerns. Ultimately, it limits the chilling effects of online learning monitoring through enhancing the exercising of data protection rights. The paper proceeds as follows: First, we outline the existing research on online learning and the application of technologies in education, focusing on learning analytics and privacy both pre- and during the COVID-19 pandemic (Section B). Next, in Section C, we examine how a commons could help support data subjects in protecting their personal data, exploring how a data protection-focused data commons could apply to online learning and how our study will assess this (Section D). In Section E, we develop an application that puts the commons into practice and conduct a study to explore the application's usefulness for supporting students' agency. We share our findings in Section F. Finally, we discuss areas of future work in Section G and explore how a data protection-focused data commons can be adapted further.

B. Background

I. Education data and online learning

3 Technology and education have long been integrated. From e-mails to using laptops in the classroom, technology has allowed for more flexible and inclusive ways of learning while introducing new methods for collaboration and information sharing.[2] However, technological developments have also increased the responsibilities that institutions have over student data, expanding and blurring the lines of what education data entails. Borgman describes education data as "grey data", where teaching, learning, and administration activities have fallen within the remit of data collected by institutions.[3] As a result, Borgman argues that it has become more difficult to assess the risks and responsibilities associated with data collection, where the privacy frontier for institutions spans open access practices, uses and misuses of data, and curating data for privacy protection.

4 The digitalisation of education has resulted in greater data collection, storage, and analysis through learning analytics. While learning analytics can help institutions understand student engagement, improve teaching, and the overall student experience,[4] they have similar characteristics to big data and so have similar data protection concerns, particularly regarding relationships between universities and students.[5] As a result, in considering a data

* Janis Wong works at the School of Computer Science, University of St Andrews and the The Alan Turing Institute, United Kingdom; Lea Racine and Tristan Henderson work at the School of Computer Science, University of St Andrews and Kirstie Ball works at the School of Management, University of St Andrews.

1 European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) L119 Official Journal of the European Union 1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

2 Neil Gordon, 'Flexible Pedagogies: technology-enhanced learning' (2014) 01 Advance Higher Education 1.

3 Christine L Borgman, 'Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier'(2018) 33(2) Berkeley Technology Law Journal 365.

4 JISC, 'Learning analytics' (15 June 2021) https://www.jisc.ac.uk/learning-analytics accessed 19 June 2022.

5 Andrew Cormack, 'A Data Protection Framework for

protection framework for governing learning analytics, Cormack argues that there should be two key stages for protecting student data.[6] Firstly, there should be greater ethical care on the discovery of significant patterns and must include safeguards for individuals' interests and rights. Secondly, applying those patterns to meet the needs of individuals requires their informed consent or a contractual agreement. Prinsloo and Slade further create a framework to support learner agency,[7] recognising that it is impossible for individuals to comprehend the scope of data that might be collected, analysed, and used and its implications when it comes to learning analytics.[8] This framework includes contextual integrity of privacy and data, student agency and privacy self-management, rethinking consent, and employing nudges. Similarly, Sclater develops a learning analytics code of practice, with a methodology for setting up appropriate governance structures, developing a taxonomy of the issues, drafting the code, consulting stakeholders, and embedding it within institutions.[9] Models that incorporate privacy-by-design have also been considered essential to learning analytics systems development, where the learning analytics design space can address issues of privacy, identify means to control data, and support trust between education stakeholders.[10]

5 As education technology becomes more commonplace, HEIs have to identify and manage the challenges around the increase of data collection, analysis, and management. Given that the authors are based in the UK, we contextualise our assessment of the online learning landscape in the country. For example, organisations such as the Joint Information Systems Committee ("JISC") and the Office for Students ("OfS") have provided guidance and supported the creation of education digital infrastructure, services, and learning providers. These include reports on learning analytics,[11] lecture recordings,[12] and supporting students with disabilities.[13] HEIs also employ data protection officers and research archivists to meet regulatory requirements.

1. COVID-19 and the impact on education

6 During the COVID-19 pandemic, the digitalisation of higher education increased significantly, with many institutions moving all of their teaching, research, and administration services online. This required students, staff, and academic institutions to rely on technologies and platforms to deliver classes and record sessions. Although some in-person sessions have resumed, blended or hybrid forms of learning remain.[14] While HEIs have done their best to ensure that online learning is conducted in a safe and secure manner, the digitisation of higher education has resulted in more data-related harms. From 'Zoom-bombing' (where a person joins a Zoom meeting uninvited and aims to disrupt the session)[15] to monitoring,[16] students have been negatively impacted by these new

Learning Analytics' (2016) 3 Journal of Learning Analytics 91.

6 Ibid.

7 Paul Prinsloo and Sharon Slade, 'Student vulnerability, agency, and learning analytics: An exploration' (2016) 3 Journal of Learning Analytics 159.

8 Paul Prinsloo and Sharon Slade, 'Student Consent in Learning Analytics: The Devil in the Details?'in Jaime Lester and others (eds), Learning Analytics in Higher Education: Current Innovations, Future Potential, and Practical Applications (Routledge July 2018) http://oro.open.ac.uk/55361/.

9 Niall Sclater, 'Developing a Code of Practice for Learning Analytics' (2016) 3 Journal of Learning Analytics 16.

10 Tore Hoel and Weiqin Chen, 'Privacy-Driven Design of Learning Analytics Applications: Exploring the Design Space of Solutions for Data Sharing and Interoperability' (2016) 3 Journal of Learning Analytics 139.

11 Niall Sclater and Paul Bailey, 'Code of practice for learning analytics' (15 August 2018) https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics accessed 19 June 2022.

12 JISC, 'Recording lectures: legal considerations' (29 July 2020) https://www.jisc.ac.uk/guides/recording-lectures-legal-considerations accessed 19 June 2022.

13 Office for Students, 'Beyond the bare minimum: Are universities and colleges doing enough for disabled students?' (18 October 2019) https://www.officeforstudents.org.uk/publications/beyond-the-bare-minimum-are-universities-and-colleges-doing-enough-for-disabled-students/ accessed 19 June 2022.

14 Arthi Nachiappan and Constance Kampfner, 'Just three top universities offer full in-person teaching this term' (20 September 2021) https://www.thetimes.co.uk/article/three-top-universities-offer-full- in- person- teaching-this- term-sheffield-sussex-southampton-covid-wwskqpcxj accessed 19 June 2022.

15 BBC, "Zoombombing' targeted with new version of app' (23 April 2020) https://www.bbc.co.uk/news/business-52392084 accessed 19 June 2022.

16 Chris Stokel-Walker, 'Universities are using surveillance software to spy on students' (15 October 2020) https://www.wired.co.uk/article/university-covid-learning-student-monitoring accessed 19 June 2022.

technologies, resulting in potential harms that impact their lives beyond academia.

2. Data protection concerns in context of online learning

7 Education and online learning fall under the remit of the data protection regulations such as the GDPR and the UK's Data Protection Act 2018,[17] where HEIs must comply with data protection laws when it comes to collecting and processing students' and staff's personal data. While there are slight differences between the two regulations, those that pertain to education and online learning remain the same. In this section, we identify the relevant parts of the GDPR that enable us to consider how data protection regulation is applied in practice in an education context for our study beyond a legal and conceptual basis. The GDPR enshrines data protection as a fundamental right and provides data subjects with rights to exercise against data controllers but does not explicitly provide instructions on how to do so. These data subject rights include the right of access by the data subject (Article 15, the right to obtain confirmation and access to several categories of information from data controllers about whether the processing of their personal data occurred), the right to be forgotten (Article 17, the right to obtain from the controller the erasure of personal data), the right to data portability (Article 20), and the right not to be subject to a decision based solely on automated processing (Article 22). While the GDPR was implemented in recognition of rapid technological developments, the Regulation aims to be technologically neutral and not depend on the techniques for the protection of natural persons (Recital 15). Instead, the GDPR has introduced qualified duties to principles such as Data Protection by Design ("DPbD"), transparency, accountability, and fairness to ensure that data protection is considered when it comes to the use, development, and deployment of technologies for data collection, processing, and sharing. In addition to data subject rights, the GDPR also requires data controllers to clearly state the lawful basis on which personal data is being processed (Article 6). These lawful bases include consent, contract, legal obligation, vital interests, public interests, and legitimate interests.

8 During online learning in the pandemic, schools across Europe have breached the GDPR. In Norway, two schools were fined as they failed to carry out a data protection impact assessment and implement adequate security when teachers asked students to download the exercise app Strava for physical education classes.[18] In Sweden, a school trialled facial recognition technologies to monitor student attendance and was fined because the data protection authority argued that consent cannot apply as students and their guardians could not freely decide if the children wanted to have their biometric data monitored.[19] In the Czech Republic, a public university was inspected as it required personal data from student applicants without a sufficient legal basis following GDPR Article 6(1) and Article 13.[20] An ongoing case in Germany also touches upon whether teachers need to give consent for live-streamed lessons in context of GDPR Article 6.[21] These cases all raise the question as to how schools and students can be supported when it comes to data protection regulatory compliance.

9 In addition to challenges related to compliance, individuals may not be able to fully realise the rights they have as data subjects. The establishment of data protection regulation that limit potential harms in an attempt to rebalance power between citizens and the companies that collect their data is a

17 United Kingdom, 'Data Protection Act' (2018) 1 Act of Parliament 1 https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.pdf.

18 Datatilsynet, 'Ålesund Municipality v Norwegian Supervisory Authority (Datatilsynet)' (2021)20/02147-6 KBK/- Norwegian Supervisory Authority https://www.datatilsynet.no/en/news/2021/alesund-municipality-fined-for-use-of-strava/

19 Datainspektionen, 'Supervision pursuant to the General Data Protection Regulation (EU) 2016/679– facial recognition used to monitor the attendance of students' (2019) DI-2019-2221 Swedish Data Protection Authority https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used- to-monitor-the-attendance-of-students.pdf.

20 Úˇrad pro ochranu osobních údaju˚ , 'Kontrola zpracování osobních údaju˚ v rámci pˇrijímacího ˇrízení na vysokou školu' [2020] Czech Data Protection Authority https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-v-ramci-prijimaciho-rizeni-na-vysokou-skolu/ds-6252/archiv=0&p1=5649.

21 CJEU, 'Case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium, Opinion of Advocate General Campos Sánchez-Bordona' (2022) 1 CJEU Preliminary Ruling 1 https://curia.europa.eu/juris/document/document.jsf?text=&docid=266121&pageIndex=0& doclang=en&mode=lst&dir=&occ=first&part=1.

step in the right direction. However, it results in the responsibilisation of data protection from data controllers to data subjects,[22] where individuals have the burden of protecting their own personal data by exercising their rights as opposed to data controllers themselves.[23] Further, the focus on individual protections and safeguards disregards the power imbalance that lies between users as data subjects and the large corporations as data controllers.[24] Individual data subjects have to exercise their rights against data controllers who are protected by institutional adoption of data protection law and any protest against the data controller's actions requires filling complaints towards the relevant Data Protection Officer. Given that individuals and groups of individuals are impacted by data-related harms,[25] it is important to examine whether data protection in practice can empower individual and collective groups of students to engage in and collaborate on data protection solutions in educational settings.[26]

10 As existing research on data protection and online learning already addresses the GDPR's application in legal terms, we focus our paper and study on the legal terms in application and practice with regards to online learning. Specifically, we examine tutorial recording given its ubiquity as part of the online learning process, which we discuss in the subsequent sections of our literature review in context of the wider online learning ecosystem.

II. Online learning technologies, privacy, and surveillance

11 Institutions such as the Open University have long run courses with a strong online component[27]demonstrating how implementing online learning technologies can improve the educational experience with clear communication of how student data are used.[28] The rapid integration of new technologies for remote learning raises the possibility of data protection harms, introducing new concerns related to online learning and privacy. For example the data protection risks emerging from the use of online platforms, such as Zoom or Microsoft Teams, include the allocation of roles and responsibilities of stakeholders, transparency of data processing and possibility to effectively exercise data subjects' rights, extra-EU data transfers, and the challenges of e-proctoring systems.[29] Universities' adoption of cloud computing also has implications beyond individuals' privacy, with questions of academic independence and integrity.[30]The data protection challenges that arise in the specific areas of lecture and tutorial recordings, e-proctoring, and platform ecosystems are discussed below.

1. Lecture and tutorial recordings

12 The usefulness of lecture and tutorial recordings has been questioned, despite their common use in online learning.[31] For students, recording viewings show no significant relationship with attainment whilst factoring in attendance, and viewings

22 Rene Mahieu, Hadi Asghari, and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (GigaNet (Global Internet Governance Academic Network) Annual Symposium 2017, December 2017).

23 Jef Ausloos and Pierre Dewitte, 'Shattering one-way mirrors — data subject access rights in practice' (2018) 8(1) International Data Privacy Law 4.

24 Lilian Edwards, 'Data Protection: Enter the General Data Protection Regulation' in Lilian Edwards (ed), Law, Policy and the Internet (Hart Publishing 2018).

25 Anuj Puri, 'A theory of group privacy' (2021) 30(3) Cornell Journal of Law and Public Policy 477 https://community.lawschool.cornell.edu/jlpp/jlpp-issue-archives/volume-30-number-3/.

26 Janis Wong, Tristan Henderson, and Kirstie Ball, 'Data protection for the common good: Developing a framework for a data protection-focused data commons' (2022) 4 Data & Policy 1.

27 Department of Education, 'Realising the potential of technology in education' (3 April 2019) https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education accessed 19 June 2022; Thomas Perry, 'The pandemic has made educators move to remote learning at an unprecedented scale – research concludes that might not be a bad thing' (3 April 2019) https://www.birmingham.ac.uk/news/latest/2020/09/the-pandemic-has-made-educators-move-to-remote-learning-at-an-unprecedented-scale.aspx accessed 19 June 2022.

28 The Open University, 'Student Policies and Regulations' (1 July 2020) https: //help.open.ac.uk/documents/policies/privacy-notice accessed 19 June 2022.

29 Chiara Angiolini and others, 'Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education' (2020) 1(1) Opinio Juris in Comparatione Studies in Comparative and National Law.

30 Tobias Fiebig and others, 'Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds' (2021) abs/2104.09462 CoRR https://arxiv.org/abs/2104.09462.

31 Tutorials are a period of study with a tutor involving one student or a small group.

may not compensate for the impact that low attendance has on attainment.[32] Additionally, the reuse of recordings may not be clarified to students. A student at a US university only found out that the professor delivering their online class had died two years earlier when the student tried to email them during the pandemic.[33] This may raise copyright issues related to the reuse of teaching materials. Taken to the extreme, recordings may also potentially cause political harm for individuals if the risks of online learning data and recordings are not properly managed, with institutions choosing not to record tutorials discussing sensitive political topics.[34] In context of data protection, when we reviewed the data protection policy that pertains to online learning at the HEIs, we found that consent was the lawful basis for tutorial recording. Given the power imbalances between students and HEIs, there may also be limitations of meaningful and informed consent both within[35] and outwith[36] educational contexts. In particular, the impact of such data processing is important to consider from a students' perspective given that tutorial recording may be presented by HEIs as a choice that students have as to whether they want to consent to be recorded, raising ethical issues when consent is relied upon as the lawful basis for data collection.

2. E-proctoring

13 E-proctoring, or the use of virtual proctoring software to monitor students through webcams, microphones, and other tracking tools with the aim of preventing cheating, has also become more commonplace. The use of e-proctoring technologies could harm agency and trust,[37] as the surveillance environment created is counter-productive to learning.[38] Other concerns include the added stress of being monitored,[39] the software being incompatible with devices,[40] and the time taken to implement it.[41] It is also unclear whether proctoring can achieve its purpose in preventing cheating.[42] In one example, a student exercised their GDPR Article 15 right of access to see what data the proctoring software was gathering about them. They found that many incidents flagged as "audio level in the room was above threshold" and "the test taker looked away from the exam page" were full of false positives, especially when staff turned up the sensitivity settings.[43] Algorithmic test proctoring

32 Martin R Edwards and Michael E Clinton, 'A study exploring the impact of lecture capture availability and lecture capture usage on student attendance and attainment' (2019) 77 Higher Education.

33 Aaron Ansuini, Tweet from January 2021 < https://twitter.com/AaronLinguini/status/1352009211501289472> accessed 20 September 2022.

34 Hong Kong Free Press, 'UK university tells lecturers not to record classes about Hong Kong and China, citing security law risks' (10 May 2021) https://hongkongfp.com/2021/05/10/uk-university-tells-lecturers-not-to-record-classes-about-hong-kong-and-china-citing-security-law-risks/ accessed 19 June 2022.

35 Prinsloo and Slade, 'Student Consent in Learning Analytics: The Devil in the Details?' (n 8); Ekaterina Muravyeva and others, 'Exploring solutions to the privacy paradox in the context of e- assessment: informed consent revisited' [2020] Ethics and Information Technology <https://link.springer.com/article/10.1007%2Fs10676-020-09531-5>; Batya Friedman, Peyina Lin, and Jessica Miller, 'Informed consent by design' [2005] Security and Usability 495.

36 Schraefel mc and others, 'The Internet of Things: Interaction Challenges to Meaningful Consent at Scale' (2017) 24(6) Interactions 26 <https://doi.org/10.1145/3149025>; Christine Utz and others, '(Un)informed Consent' [2019] Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security <http://dx.doi.org/10.1145/3319535.3354212>; Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' (Serge Gutwirth and others eds, Springer Netherlands 2009).

37 Todd Feathers, 'Colleges Say They Don't Need Exam Surveillance Tools to Stop Cheating' (16 November 2020) https://www.vice.com/en/article/88ag8z/colleges-say-they-dont-need-exam-surveillance-tools-to-stop-cheating accessed 19 June 2022.

38 Zeynep Tufecki, 'The Pandemic Is No Excuse to Surveil Students' (4 September 2020) https://www.theatlantic.com /technology/archive/2020/09/pandemic-no-excuse-colleges-surveil-students/616015/ accessed 19 June 2022.

39 Colleen Flaherty, 'Big Proctor' (11 May 2020) https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19 accessed 19 June 2022.

40 Rebecca Heilweil, 'Paranoia about cheating is making online education terrible for everyone' (4 May 2020) https: //www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence accessed 19 June 2022.

41 Jane C Hu, 'Paranoia about cheating is making online education terrible for everyone' (6 October 2020) https://slate.com/technology/2020/10/online-proctoring-proctoru-proctorio-cheating-research.html accessed 19 June 2022.

42 Lindsey Barrett, 'Rejecting Test Surveillance in Higher Education' (2021) 1(1) Michigan State Law Review (forthcoming).

43 Gabriel Geiger, 'Students Are Easily Cheating 'State-of-the-Art' Test Proctoring Tech' (3 May 2021) >https://www.vice.com/en/article/3an98j/students-are-easily-heating-state-of-the-art-test-proctoring-tech< accessed 19 June 2022.

may also discriminate based on gender and race.[44] The use of proctoring services was condemned by UK Bar professional training course students, where students were monitored using webcams throughout the examination without any breaks and moving away from the webcam would result in automatic termination.[45] No change to the online exams were made despite one third of exams being affected by technical difficulties.[46]

3. Platform ecosystems

14 The data protection considerations of tools and the usefulness of lecture and tutorial recordings have also been questioned. Many tools used by HEIs to deliver online learning (such as Zoom and Microsoft Teams) were not created for education. As a result, these third-party companies may be less sensitive to stakeholders' motivations, where students are treated as consumers, without regard to their participation in education.[47] For example, the Microsoft Office Productivity Score included in Microsoft Teams tracks the time and activity of its users, producing data on the extent to which individuals are working on its platform. Initially, this data could be accessed by institutions and linked to specific usernames. Even if HEIs do not access this data, it could still be collected by digital platforms and may be shared and sold to third parties. Only after privacy concerns were raised did Microsoft remove usernames and change how the data gathered are presented.[48] Particularly where universities are public institutions, these data processing practices should be made transparent to those who use these technologies.

III. Solutions

15 In response to some of the digital and data-related challenges that have arisen from COVID-19, many organisations have looked at the impact of the pandemic on education. The OfS engaged stakeholders to produce guidance establishing the essential components of successful digital teaching and learning, recommending core practices HEIs can use to improve online learning for students.[49] JISC have written a report to understand the COVID-19 response and explore the future of digital learning and teaching.[50] Policy solutions were also devised for identifying the future role of emerging technologies in education and training.[51] The Open Data Institute has also suggested public engagement to support data governance considerations when working with online learning data.[52]

16 More broadly, the UK Information Commissioner's Office established a code to help employers comply with the GDPR and to encourage them to adopt good practices, including monitoring at work.[53] The UK Department for Education created a COVID-19 addendum to acknowledge issues of privacy

44 Shea Swauger, 'Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education' [2020] Hybrid Pedagogy https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/ accessed 19 June 2022.

45 Neil Rose, 'Bar students urge online exams rethink' (2 June 2020) https://www.legalfutures.co.uk/latest-news/bar-students-urge-online-exams-rethink accessed 19 June 2022.

46 Bar Standards Board, BSB announces new opportunities to sit Bar Professional Training Course (BPTC) exams (11 September 2020) https://www.barstandardsboard.org.uk/resources/press-releases/bsb-announces-new-opportunities-to-sit-bar-professional-training-course-bptc-exams.html accessed 19 June 2022.

47 Joseph Duball, 'Shift to online learning ignites student privacy concerns' (28 April 2020) https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/ accessed 19 June 2022.

48 Jared Spataro, 'Our commitment to privacy in Microsoft Productivity Score' (1 December 2020) https://www.microsoft.com/en-us/microsoft-365/blog/2020/12/01/our-commitment-to-privacy-in-microsoft-productivity-score/ accessed 19 June 2022.

49 Office for Students, 'Gravity assist: propelling higher education towards a brighter future' (1 March 2021) https://www.officeforstudents.org.uk/publications/gravity-assist-propelling-higher-education-towards-a-brighter-future/executive-summary/accessed 19 June 2022.

50 JISC, 'Learning and teaching reimagined: a new dawn for higher education?' (4 November 2020) https: //www.jisc.ac.uk/reports/learning-and-teaching-reimagined-a-new-dawn-for-higher-education accessed 19 June 2022.

51 Riina Vuorikari, Yves Punie, and Marcelino Cabrera Giraldez, 'Emerging technologies and theteaching profession' [2020] J RC Science for Policy https://publications.jrc.ec.europa.eu/repository/ handle/JRC120183.

52 Open Data Institute, ODI Fellow Report: Data governance for online learning (7 September 2021) https://theodi.org/article/data-governance-online-learning/ accessed 19 June 2022.

53 Information Commission's Office, 'The employment practices code' (1 November 2011) https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf accessed 19 June 2022.

in schools.[54] The European Commission also identified the need to create a trusted digital education ecosystem with high-quality content, user-friendly tools, value-adding services and secure platforms that maintain privacy and uphold ethical standards as part of its new Digital Education Action Plan.[55]

1. Collaborative solutions in theory and in practice

17 In supporting more inclusive and equitable online learning practices, researchers and practitioners have shared their experiences of online learning during the pandemic.[56] The shift to online learning introduces new questions around the ethics of care related to online and remote work.[57] The Centre for Research in Digital Education created the Manifesto for Online Learning to illustrate how surveillance culture can be resisted.[58] Silverman et al. share their lessons on helping staff transition to authentic assessments without e-proctoring.[59]

18 Collaboration with students can also support increased agency and trust both in the data protection process as well as with their institutions. Plunkett et al. find that to ensure that student privacy frameworks align with students' digital practices and privacy expectations, adult stakeholders should incorporate robust ways for youth to participate in discussions about tackling student data privacy challenges.[60] Teachers have mentioned the importance of students voicing concerns about the use of novel technologies in education.[61] Addressing how this can be done, JISC suggests that universities prioritise blended learning approaches where possible, and that students co-design curricula.[62] Williamson and Hogan recommend that higher education stakeholders should work collegially to define alternative imaginaries that can guide post-pandemic recovery of HEIs, moving away from using academia as an engine for producing measurable learning performance and associated workforce productivity gains.[63] Co-created solutions as a response to the pandemic to navigate privacy and security during online learning were also crowd-sourced such as the Coronavirus Tech Handbook[64] and A Comprehensive Guide To Tech Ethics and Zoom Class.[65]

C. Co-creating solutions for protecting students' data

19 Given the importance of co-created and collaborative solutions, our study investigates whether creating a socio-technical data protection-focused data commons for online learning can protect students' personal data by providing them with more agency to

54 Department of Education, 'Safeguarding and remote education during coronavirus (COVID-19) (10 March 2021) https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19#virtual-lessons-and-live-streaming accessed 19 June 2022.

55 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digital Education Action Plan 2021-2027 Resetting education and training for the digital age' (30 September 2020) https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624#document1 accessed 19 June 2022.

56 Ben Williamson, Rebecca Eynon, and John Potter, 'Pandemic politics, pedagogies and practices: digital technologies and distance education during the coronavirus emergency' (2020) 45(2) Learning, Media and Technology 107 https://doi.org/10.1080/17439884.2020.1761641.

57 Marianna Fotaki, Gaz Islam, and Anne Antoni, Business Ethics and Care in Organizations (Routledge 2019).

58 Siân Bayne and others, The Manifesto for Teaching Online (MIT Press 2020).

59 Sarah Silverman and others, 'What Happens When You Close the Door on Remote Proctoring? Moving Toward Authentic Assessments with a People-Centered Approach' (2021) 39(3) Educational Development in the Time of Crises.

60 Leah Plunkett, Urs Gasser, and Sandra Cortesi, 'Student Privacy and the Law in the Internet Age' [2021] The Oxford Handbook of U.S. Education Law https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190697402.001.0001/oxfordhb-9780190697402-e-30.

61 Monica Chin, 'An ed-tech specialist spoke out about remote testing software — and now he's being sued' (22 October 2020) https://www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus accessed 19 June 2022.

62 Paul Feldman, 'Education and research improves lives, and technology improves education and research' (1 November 2020) https://www.foundation.org.uk/getattachment/8803ab67-86b4-4657-9dae-733a253e4741/paul-feldman-slides-pdf.pdf accessed 19 June 2022.

63 Williamson, Eynon, and Potter (n 61).

64 Newspeak House, 'Coronavirus Tech Handbook' (20 March 2020) https://coronavirustechhandbook.com/ accessed 19 June 2022.

65 70Mehitabel Glenhaber, 'A comprehensive guide to tech ethics and Zoom' (18 November 2020) https://sourceful.us/doc/652/a-comprehensive-guide-to-tech-ethics-and-zoom accessed 19 June 2022.

exercise their data protection rights.

20 Developed by Elinor Ostrom, the commons considers collective action, trust, and cooperation through design principles.[66] The commons guards a common-pool resource ("CPR"), a resource system that is sufficiently large as to make it costly to exclude potential beneficiaries from obtaining benefits from its use and may be over-exploited. The CPR enables "transparency, accountability, citizen participation, and management effectiveness" where "each stakeholder has an equal interest".[67] Central to governing the commons is recognising polycentricity, a complex form of governance with multiple centres of decision-making, each operating with some degree of autonomy.[68] The norms created by the commons are bottom-up, focusing on the needs and wants of the community and collectively discussing the best way to address any issues.[69]

I. Education as a commons

21 Adapting the commons to individuals' collective digital data, Hess and Ostrom developed the knowledge commons, where knowledge is the CPR.[70] As new technologies enable information capture, the knowledge commons recognises that information is no longer a free and open public good and now needs to be managed and protected for archival sustainability and accessibility. Crucially, the commons addresses data-related governance challenges that arise due to spillovers created by the reuse of data, thereby increasing its value over time.[71]

22 An example of a knowledge commons is a university research repository.[72] Developing a university repository requires multiple layers of collective action, coordination, and shared information and expertise. Academics and researchers can contribute to the repository as the more it is used, the more efficient it is to the university. Others outside that community can browse, read, and download the repository, further enhancing the quality of its resources. By breaking down large, complex, collective action problems into action spaces through the Institutional Analysis and Development ("IAD") framework,[73] collective action problems can be assessed so that institutions can more accurately meet the needs of the community, including how information, knowledge, and data can be used to serve the common good.[74]

23 The commons has been further adapted to the university environment. Madison illustrates that as universities continue to evolve, the nature of the university may change from a knowledge to a data-oriented institution, resulting in the conflation of data as knowledge.[75] As a result, the way institutions may be governed could also change. In order for HEIs to manage their resources for maximum benefit and minimal social and private harm, HEIs could consider the knowledge commons to examine data governance beyond intellectual property rights and be open to multi- stakeholder engagement when creating university policies and meeting third-party obligations for education data. Although the risks of data collection, sharing, and security are not explored, Madison offers insights into how university data could be managed as a commons via strategies of openness, sharing,

66 Elinor Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action (Cambridge University Press 1990).

67 Charlotte Hess, 'Research on the Commons, Common-Pool Resources, and Common Property' [2006] Indiana University Digital Library of the Commons http://dlc.dlib.indiana.edu/dlc/contentguidelines.

68 Vincent Ostrom, Charles M Tiebout, and Robert Warren, 'The organization of government in metropolitan areas: a theoretical inquiry' (1961) 55 American Political Science Review 831.

69 Elinor Ostrom, The Future of the Commons: Beyond Market Failure & Government Regulations (Institute of Economic Affairs 2012).

70 Charlotte Hess and Elinor Ostrom, Understanding Knowledge as a Commons: From theory to practice (MIT Press 2007).

71 Diane Coyle, 'Common governance of data: appropriate models for collective and individual rights' (30 October 2020) https://www.adalovelaceinstitute.org/blog/common-governance-of-data/ accessed 19 June 2022.

72 Hess and Ostrom (n 75).

73 Elinor Ostrom, Understanding Institutional Diversity (1st edn, Princeton University Press 2005).

74 Michael D McGinnis, 'The IAD Framework in Action: Understanding the Source of the Design Principles in Elinor Ostrom's Governing the Commons' in Daniel Coleand and Michael D McGinnis (eds), Elinor Ostrom and the Bloomington School of Political Economy, Volume 3: A Framework for Policy Analysis (Lexington 2018) https://polisci.indiana.edu/documents/profiles/mcginnis1.pdf.

75 Michael J Madison, 'Data governance and the emerging university' in Research Handbook on Intellectual Property and Technology Transfer (Edward Elgar Publishing 2020) https://www.elgaronline.com/view/edcoll/9781788116626/9781788116626.00027.xml.

and polycentricity, but with contextually-appropriate elements of proprietary management and exclusivity with regards to intellectual property.

24 As a result, in order to increase student agency in protecting their personal data, a commons could be created to support collaborative means for them to meet their data protection preferences with the knowledge of their institutions' data protection practices and of their individual data protection rights.

II. A commons for online learning

25 A data protection-focused data commons allows data subjects to collectively curate, inform, and protect each other and the collective exercise of data protection rights. A commons that focuses on data protection can provide students with agency over their personal data and redress the power imbalance between them and HEIs. For students, participating in the commons allows them to improve their understanding of their institution's policy and external organisations' guidance when it comes to collecting, processing, and sharing their online learning personal data. The commons also allows them to ask questions to experts, raise any questions about data protection to other students, review their consent decisions on tutorial recordings, and exercise their data protection rights. It simplifies the data protection rights procedures by including information, instructions, and templates on how rights should be collectively exercised, giving data subjects an opportunity to engage with and shape the data protection practices that govern how their personal data are protected.

26 Creating a data protection-focused data commons could help identify how much understanding and control data subjects have over their personal data, supporting them in choosing their data protection preferences. A commons for data protection does not require the creation of a new legal framework, but rather, operates within the current data infrastructures used by data subjects and acknowledges the limitations of existing laws, technologies, and policies that steward data. Thus, the focus on data protection as part of the data commons shifts data protection responsibilities away from the individual alone to their community, where knowledge, expertise, and experiences can be pooled together to identify working solutions. Although personal data are still kept personal and private, the collaborative nature of sharing, discussion, and advising on data protection problems opens up potential options for everyone to support informed decision-making and achieving data protection preferences through a data commons.

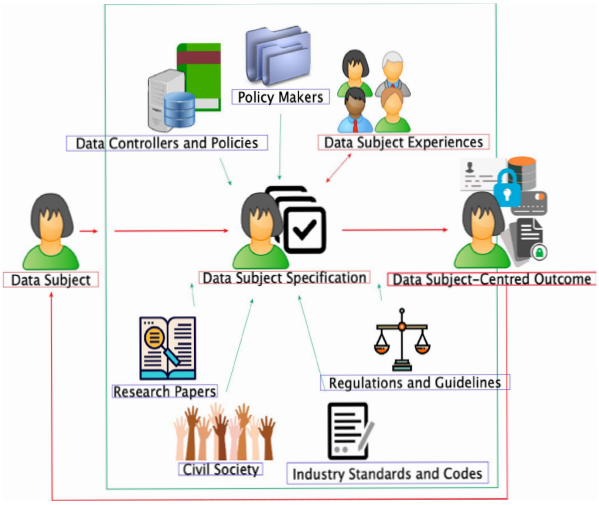

Figure 1: In a data protection-focused data commons (green), the data subject specifies to what extent they would like their data to be protected based on existing challenges pre-identified within the data commons for the use case (red). No prior knowledge of existing law, norms, or policies are required. Along with stakeholder information (blue), the data subject specification is then used to inform their data protection outcome as generated from the system. As the outcome is data subject-centred, decisions ensuring the protection of the data subject's personal data may override existing preferences, policies, or standards set by other stakeholders. Data subjects can return to and review their outcomes, add their data subject experiences to the data commons, and participate in the co-creation process at any time.

27 In our previous work,[76] we interviewed commons experts to assess if and how a commons framework can be applied to data protection to support the protection of data subjects' personal data. From those

76 Wong, Henderson, and Ball (n 26).

interviews, we found that collaboration across stakeholders and disciplines could overcome excluding data subjects and doubts about the effectiveness of the commons. The purpose of the commons needs to be clear because the use of the commons model is a choice, and that clarity allows for new iterations of the commons to best suit data subject needs. The commons must include the vision of communities and people about what is at stake, what it is about, how it works, and how data have been managed. Ultimately, commoning was identified as a verb, where the community has to actively participate in the development process and its application and is necessary for successful co-creation and participation. Based on these findings, we adapted an IAD framework and policy scaffolding for the creation of a data protection-focused data commons (included in Appendix A), which we now apply to create an appropriate commons for online learning.

D. Research questions

28 Our aim is to create a commons tool, an interactive resource hub that applies the commons principles, that can be used by students to support them in choosing their own online learning data protection preferences. By voicing their concerns, students risk not being able to access university teaching if they object to certain policies and practices. The use of the tool by students aims to help them understand the reasons behind tutorial recordings and help make more informed decisions about whether they choose to consent to being recorded. The tool also attempts to provide more agency, not only in how their personal data are used by the university, but also their ability to freely participate in classes. It is hoped that participation in the data protection-focused data commons will encourage the redistribution of power between students as data subjects, universities as data controllers, online learning platforms, and staff.

29 We established three research questions to examine whether an online learning data protection-focused data commons can help students regain their agency over their personal data:

- **RQ1:** Does the ability to interact with commons resources help inform students about the purposes of online learning and tutorial recordings?
- **RQ2:** How effective is the commons model for supporting user preferences for protecting their personal data?
- **RQ3:** Does the commons model encourage more transparency around data protection between data subjects, data controllers, and other involved stakeholders?

E. Methodology

30 In developing the study to address our research questions, we applied Ostrom's design principles (Section B) and the requirements illustrated by the IAD commons framework (Appendix A) to put commons theory into practice. We also incorporated Prinsloo and Slade's learner agency framework to support student agency and empowerment in the process of protecting their education data.[77]

31 To adapt the commons tool to online learning, we developed the application for Microsoft Teams, the software used by the authors' university for conducting online learning. A new Team was created for each tutorial online learning classroom environment to represent each student testing group. The tool was then uploaded as a custom application to Microsoft Teams and each tutorial Team had a working copy of the application (Figure 2).

77 Prinsloo and Slade, 'Student vulnerability, agency, and learning analytics: An exploration' (n 7).

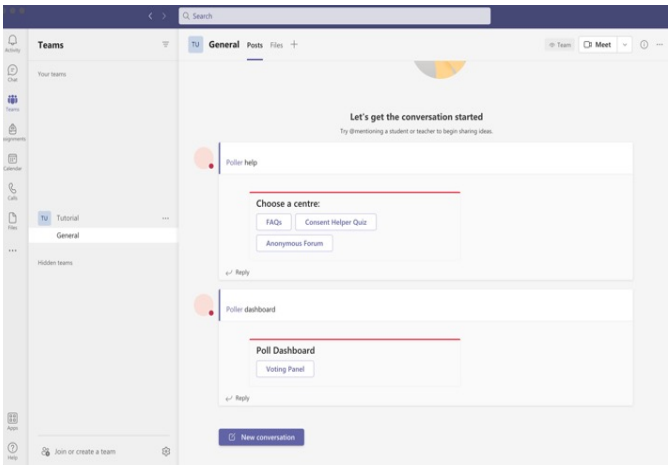

Figure 2: The commons tool, showing the help center and the consent voting panel, as it appears on Microsoft Teams.

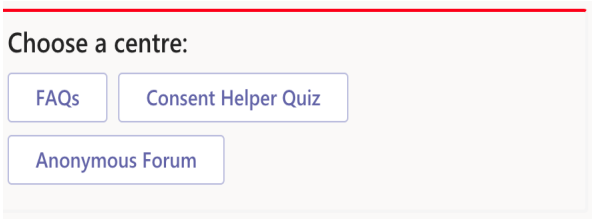

Figure 3: The commons tool help centre has three sections to help the student develop a more comprehensive understanding of the policies, laws, and guidance that governs tutorial recordings and supports them in making a decision as to whether or not they should consent to tutorial recording.

32 The commons tool was separated into two main parts. The first part, the commons help hub (Figure 3), has three sections:

- Frequently Asked Questions (FAQs) (Figure 4) provides answers to questions about polling, rights, policies, and contacts, mapping to the commons CPR principle for increased transparency and accountability as well as recognising the different levels of online learning governance (polycentricity).
- Consent Helper Quiz is a short quiz to help participants figure out whether the session should be recorded, mapping to the commons CPR principle for effective management.
- Anonymous Forum is an area for participants to share their thoughts or concerns anonymously, mapping to the commons CPR principle for citizen participation and supporting each student's equal interest. Along with the FAQs, the Forum can also support conflict resolution and reporting mechanisms following Ostrom's design principles.

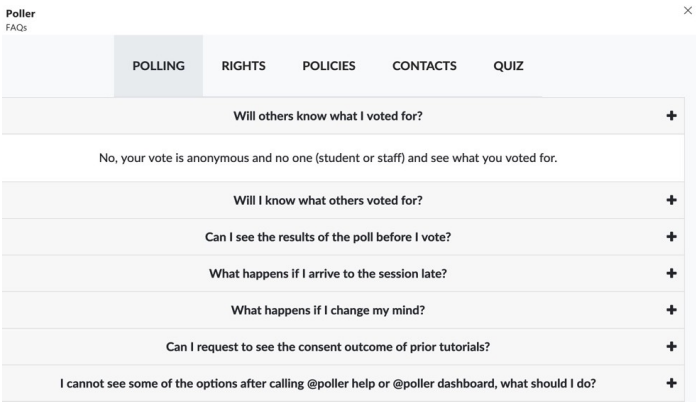

Figure 4: The FAQs contains text-based resources such as information about why tutorial recordings are happening, university data policies, external tutorial recording policies, and information on how to exercise data protection rights.

33 Within the FAQs, participants can find information about online learning, university policies, and data protection as listed below:

- Information about the tutorial recording consent Voting Panel (described in detail later in this section).
- Data protection and information regulations, e.g., the GDPR.
- Data protection rights centre.
- Information about what rights data subjects (students) have.

- Ability for students to request an anonymous record of consent poll results.
- E-mail templates for exercising data subject rights.
- How to contact a data protection expert and the DPO.
- Information about the data collected from the Consent Helper Quiz.

34 The Consent Help Quiz aims to help participants decide whether they should or should not consent to recording tutorials based on their personal preferences. All questions for the quiz have "yes" or "no" answers. Depending on the participant's answers, at the end of the quiz, the final result will display "You may not need to opt-out", "You may want to consider opting out", or "You may want to strongly consider opting out". Questions on the quiz include:

- Are you potentially revealing any sensitive personal information (racial or ethnic origin, political opinions, religious belief, genetic data, and biometric data etc.) during the session?
- Will you avoid discussing certain topics if the session is recorded?
- Will you avoid asking questions or points of clarification if the session is recorded?
- Will the session being recorded affect your likelihood of participating?
- Do you think recording the session will improve your academic study?
- Are you planning to re-watch the tutorial once it is done?
- Do you trust that the university will keep the recording safe?
- Do you trust that the platform which the session recording is taking place on will keep the recording safe?

35 The final part of the commons help hub is the Anonymous Forum (Figure 5), which allows students to share information, questions, or concerns they have about tutorial recordings.

36 The second part of the commons tool is the Voting Panel which conducts the consent poll (Figure 6).

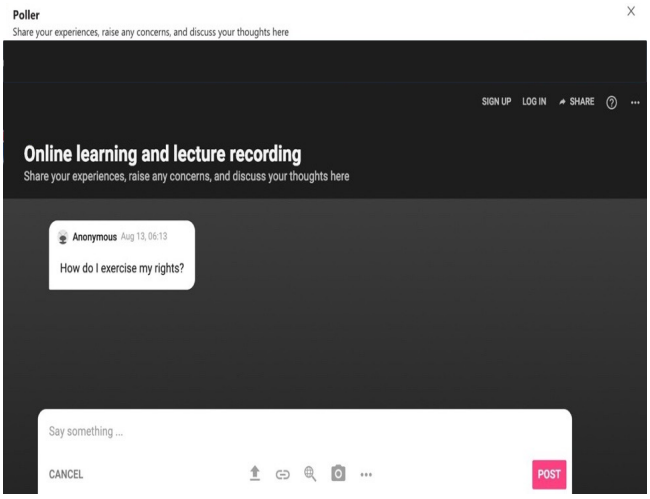

Figure 5: The Anonymous Forum is a space where students can participate anonymously in an open dialogue with other students in their tutorial about any questions that they have about tutorial recordings.

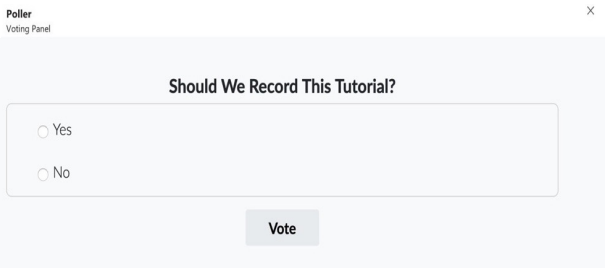

Figure 6: The Voting Panel is the consent poll where students can consent to or not consent to tutorial recording based on their own personal preferences. The poll is anonymous and the full results of the vote from the class will be displayed after voting. If everyone consents, the tutorial recorded.

I. Testing the application

37 To test the commons tool, we split the study into three parts: an entry questionnaire, an interactive task to test of the commons or control application, and an exit questionnaire. Figure 7 illustrates the different stages of the study.

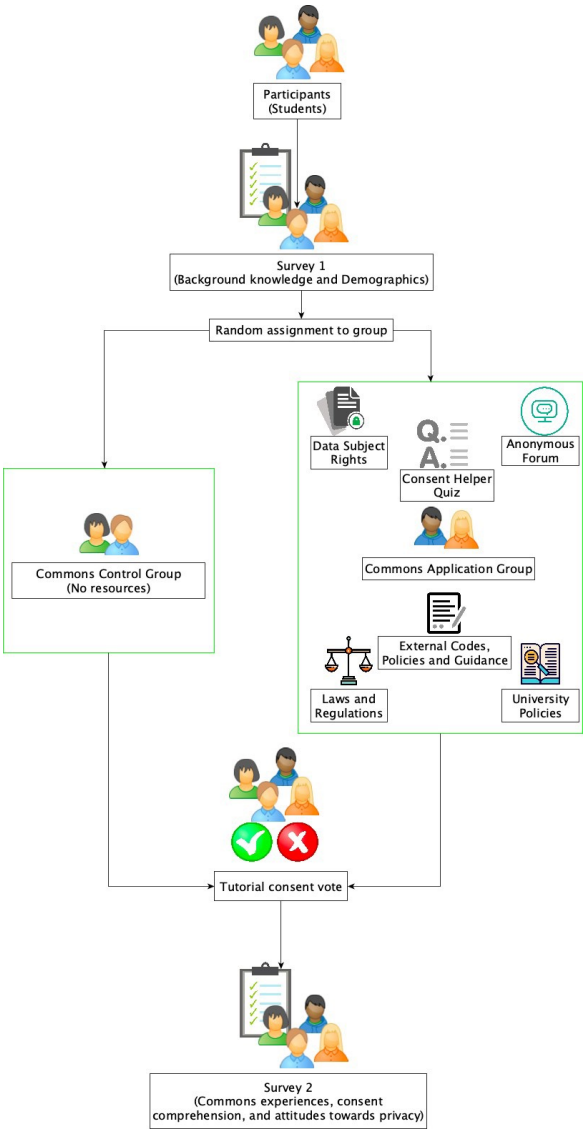

Figure 7: Study walk-through summary

38 The study was conducted online between April 2021 and October 2021. As the authors are based in the UK, all participants were undergraduate and postgraduate taught students studying at UK-based universities over 18 years of age. The study was approved by the relevant University Ethics Committee. We outline the initial survey, application testing, and final survey components below.

1. Initial survey

39 For the first part of the study, an initial survey was completed by potential participants to gather some participant information and to determine their eligibility. This assessed the level of users' knowledge of tutorial recordings, data protection, online learning, and university policies. The questionnaire also identified how participants felt about users' ability to exercise their agency with regards to tutorial recordings and online learning.

2. Testing the application

40 After the first survey was completed, we e-mailed potential participants to schedule a time for the rest of the study and include a separate document with the mock-tutorial information (Appendix B). Although 175 participants completed the initial survey, only 34 responded to our email to schedule a time to test the application. Participants were then randomly assigned to be in the control testing group or the commons application testing group on Microsoft Teams. Those in the control group were given two minutes to consent or not consent to tutorial recording. Those in the commons group were given 10 minutes to explore the resources in the application and vote. The control group only had access to the voting panel and the commons application group had access to all the resources outlined in the previous section.

3. Final survey

41 The final part of the study, the exit survey, allowed participants to reflect on their experience of the tool, identify what resources they used if they were part of the commons application testing group, attitudes towards privacy, data protection and online learning, and examine to what extent they now know about their consent and data protection options as part of online learning. The survey included Internet Users' Internet Privacy Concerns ("IUIPC")[78] questions adapted for online learning to benchmark their privacy concern levels that relate to privacy and data awareness, control, and collection

78 Naresh K Malhotra, Sung S Kim, and James Agarwal, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model' (2004) 15 Information Systems Research 336.

(Appendix C).

F. Analysis

I. Participant demographics and privacy awareness

42 34 students participated in our study. The participants studied Computer Science (6), Management (3), Finance (2), Philosophy (2), Psychology (2), and 19 other subjects that were only studied by one participant. 23 participants were undergraduates and 11 were postgraduates. Our participants predominantly identified as female (26) with seven males, and one not disclosed. From our results, we did not find any correlation between the discipline of study, level or year of study, or gender.

43 Regarding tutorial recordings, 19 participants thought that they had control over whether a tutorial was recorded, with 10 disagreeing and five were uncertain. When asked about the university's tutorial recording policy, 17 were aware that there was one, 12 were not aware, and five were unsure. Only eight had read the policy. More broadly, most students (14) were not aware of how the university processes their personal data, 10 were unsure, and 10 were aware. Most students (22) were not aware of how Microsoft Teams processed their data.

44 When asked about their online learning and tutorial recording experiences, most students (20) said that some of their tutorials were recorded. In our study, we found that 18 students said that they were asked to consent to recordings for all of their online tutorials, five said only some asked for consent, seven were not asked, and four were not sure. In considering personal experiences of online learning, 11 said that online learning made a positive impact on their educational experience, two had no impact, 12 were impacted negatively, and nine were unsure. Focusing on tutorial recordings, 13 felt that tutorial recordings were a net positive, 17 did not feel that it impacted their educational experience, two were negatively impacted, and two were unsure.

Figure 8 shows the overall level of privacy concern of our participants, based on their responses to online learning IUIPC questions (Appendix C). The higher the score, the more privacy-concerned a participant is, where 55 is the maximum score and 11 is the minimum. Existing work shows that internet use reduces IUIPC.[79] A positive relationship was found between privacy concerns and government involvement in privacy regulation,[80] suggesting higher IUIPC scores for participants governed by the GDPR. The median score for our participants is 46. While our participants were based in the UK which falls under the GDPR's remit students as young people are considered to have high levels of internet use, suggesting a relatively high level of privacy concern for their demographic. In assessing the significance of specific IUIPC questions for influencing a participant's privacy concerns, from our exploratory factor analysis (TLI of factoring reliability = 1, RMSEA index = 0, and a confidence level of 95%), we found that for data collection, participants who thought about whether they should provide personal information to universities demonstrated higher levels of privacy concern, with a correlation of 0.8. Examining the IUIPC data awareness factor, the more important participants thought it was to be aware and knowledgeable about how their personal information will be used, the higher their IUIPC score, with a correlation of 0.9.

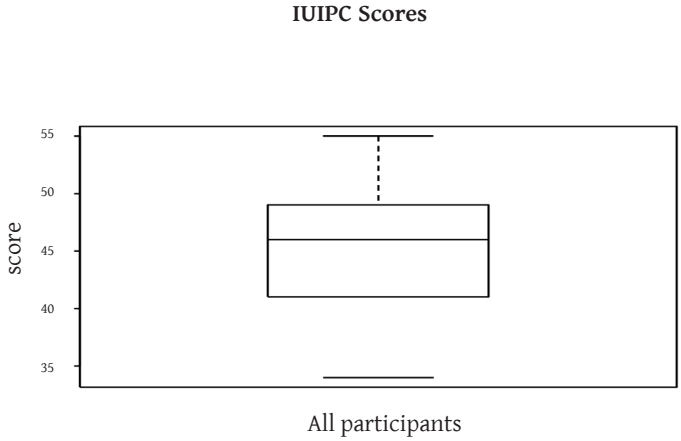

Figure 8: The IUIPC scores of study participants. The median score for our participants is 46, demonstrating a moderately high level of privacy concern, where 55 is the maximum score and 11 is the minimum.

79 Steven Bellman and others, 'International Differences in Information Privacy Concerns: A Global Survey of Consumers' (2004) 20 Inf. Soc. 313.

80 Sandra J Milberg and others, 'Values, Personal Information Privacy, and Regulatory Approaches' (1995) 38(12) Commun. ACM 65 https://doi.org/10.1145/219663.219683.

From our analysis, consent as a form of privacy control was not significant enough to be considered as a factor for assessing the level of privacy concern.

II. Consent levels for online learning

45 Figure 9 shows that most (28) participants consented to tutorial recording. We also asked participants to state whether they decided to change how they voted as a result of doing the exit survey. One participant from the commons group and two participants from the control group would change the way they voted based on the exit survey. All three changed from not consenting to giving consent. Most students (18) stated that they did not think twice before handing over their data to the university. This suggests that students may feel obliged to provide such data in order to access education and indicates a certain level of trust that students have of HEIs to use that data for academic purposes.

Several participants across both groups stated that disability and accessibility were important reasons as to why they consented to the tutorial recording. In context of the COVID-19 pandemic when the study took place, this is particularly important given the challenges students face during online learning. As a result, it is necessary to consider accessibility needs when considering whether and how tutorial recording should be conducted to support students.

Participant response to the question 'Should we record this tutorial?'

Figure 9

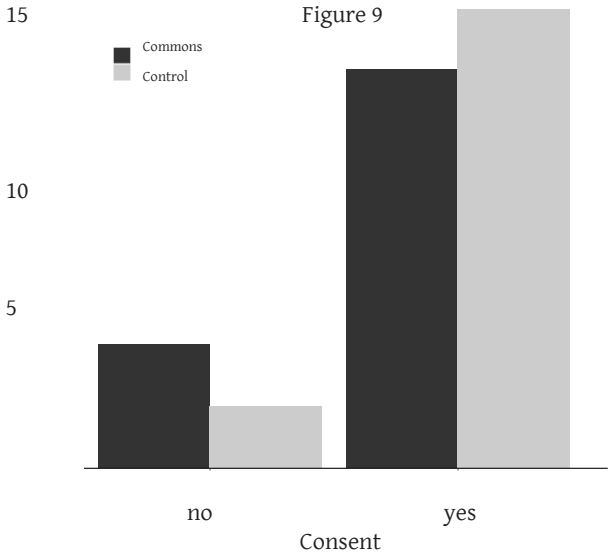

Figure 9: Consent preferences from participants answering the question "Should we record this tutorial?". The majority of participants in both commons and control groups consented to tutorial recording.

III. Commons tool: information, usefulness, and agency

46 Table 1 shows that resources related to data protection rights and policies were the most useful to our study participants. This suggests that participants are keen to increase their understanding of what protections are in place for their data and what recourse they have if anything goes wrong.

47 Interestingly, the actual consent voting poll where participants had to consent or not consent to the tutorial recording was the second least useful. This is consistent with existing literature on the limitations of meaningful and informed consent within and outside education that we outlined in Section B. This demonstrates the importance for students to feel that they are making informed choices (where the outcome is less important) in an online learning environment, where they do not necessarily question the university's motivations for recording tutorials. Additionally, given that the resources that give students more transparency were found to be marginally more useful that those that increased agency such as exercising rights and the quiz, more research could be done to examine how students believe their agency over their personal data could be increased.

Commons Resource	Count
Information on the University tutorial recording	13
The FAQs	13
Data protection law	12
Information on exercising your rights	12
The consent quiz	10
The consent voting poll	9
The anonymous forum	8

Table 1: The resources in the commons that commons group participants found useful for helping them decide whether or not they should consent to tutorial recording. All participants found at least one commons resource to be useful.

48 When elaborating on why participants found certain features of the commons useful, one student said that "I hadn't really known anything about tutorial recording policy or the laws and my rights related to these recordings before so I though (*sic*) it was interesting to learn more about my rights and more about what tutorial recordings would be used for and when they should be used". Another student thought that "the information about the University policy was very valuable to make might (*sic*) decision, and having access to it easily is helpful. The FAQs was (*sic*) definitely the most helpful element, as it answered a lot of my questions simply". A student who found the forum useful explained that: "I think I was most swayed by the anonymous student posts. Personally, I didn't want the session recorded, but I knew it would be helpful for others to review later or who had missed the session/not been mentally present due to chronic illness, etc.". Overall, nine participants in the commons group agreed that they would use the commons to improve the protection of their personal data. Five somewhat agreed, two neither agreed or disagreed, and one somewhat disagreed.

1. Control group comparison

49 When the control group, where participants did not have access to the commons resources, were asked what would have be useful for them to help them decide whether or not to consent to tutorial recordings, nine participants wanted more information. These included: "Who would be able to view and access the tutorial after it had been recorded and if it would be used for anything else other than for study use for the module.", "More information on where the recording would be stored and who it would be accessible to would be helpful.", and "Whether the lecturer could see individual responses: this would influence whether I answer yes or no as I don't want to come across as a spanner in the works". From those responses, the additional information participants would have liked fell into two categories: information about the consent voting tool and information about the tutorial recording itself. Both of these are covered under the Information on the University tutorial recording section and the FAQs section of the commons. Two participants wanted to know if turning on their webcam was required as they would not consent if it was. Eight participants did not feel that they needed more information to consent either because they did not care about being recorded, would have agreed to being recorded if they knew someone in class would need the recording, or felt that they were fully aware of the tutorial recording process.

IV. Topic, content, and attitudes towards tutorial recordings

50 When conducting the study, we asked participants to imagine that they were taking part in a mock-tutorial on conducting research on social media and provided them with the lesson plan. During their post-study survey, we asked participants whether the topic of the mock-tutorial impacted their consent levels to tutorial recording (Figure 10).

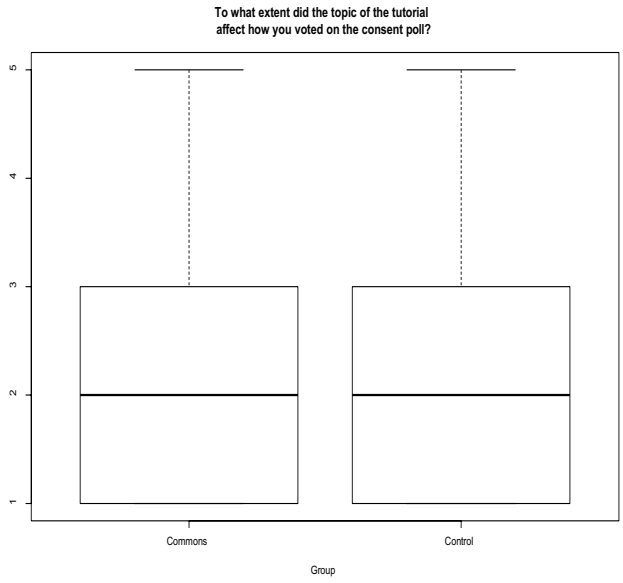

Figure 10: Impact of the tutorial topic on consenting to tutorial recording. The topic of the tutorial is not a strong factor for informing whether a student decides to consent or not consent to the tutorial recording in both commons and control groups. The median for both the commons and control group is two.

51 From the survey responses, participants suggest that they would not refuse consent based on the tutorial topic alone as it would depend on other factors such as if they felt they needed to re-watch a tutorial recording and whether the topic involves providing personal information that the participants themselves did not want to share.

52 We wanted to increase our understanding of how students participate in recorded digital classrooms and how that may impact personal information sharing. To examine this, we asked participants whether they would avoid any topics during online learning, specifically those listed as special category personal data under GDPR Article 9. From Figures 11 and 12, the high number of avoided topics during tutorial recordings suggest that even if participants consented to tutorial recordings, teaching subjects that result in the discussion of these sensitive personal data may limit student participation in online learning. Two of the highest ranked topics 'data concerning a person' (22) and 'political opinions' (20) represent a broad range of information often shared in discussions. Six commons and three control group participants did not avoid any topic. Importantly, commons participants avoided fewer topics across all categories. This suggests that because commons participants have a more comprehensive understanding of how their data are stored, they are more comfortable having discussions about matters related to the special category personal data recorded. More generally, in examining the impact of the tutorial topic and the content participants are willing to share, they explained that they would rather not participate than not consent to the tutorial recording because they had control over what they said. As a result, it is important for staff to consider how to engage with teaching sensitive topics online to maximise participation and generate the most value from online learning.

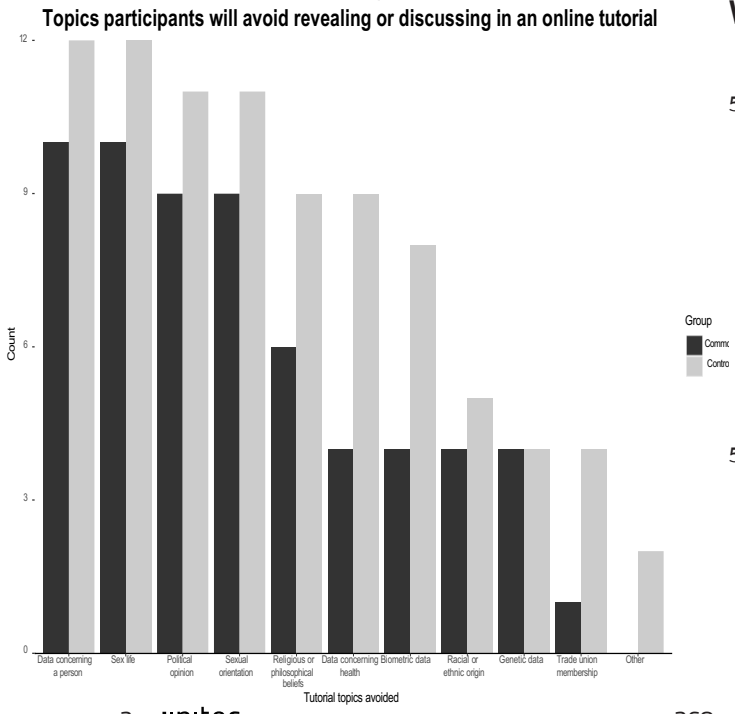

Figure 11: Topics participants avoided in a recorded online learning environment from participants answering the question "Are there topics you will avoid discussing or revealing about yourself if the tutorial is recorded compared to physical classes?". The two "other" responses include information that one participant considered to be "triggering" such as "mental health, other personal information, and financial information" as well as what another participant considered "anything that could be misconstrued or used out of context if the recording was inadvertently (or deliberately) released". Overall, the commons participants are less likely to avoid discussing certain topics.

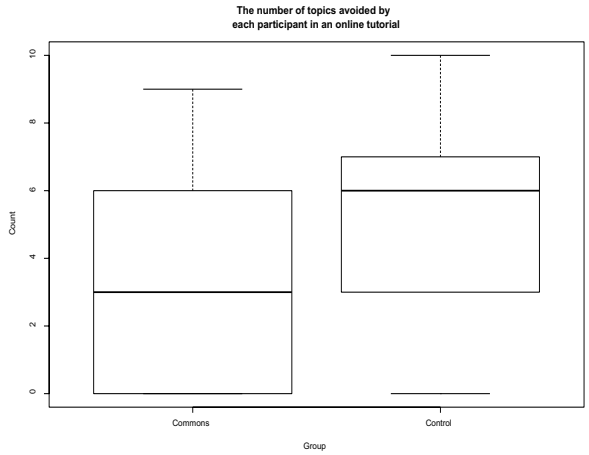

Figure 12: The number of topics avoided by each participant. Commons participants are less likely to avoid discussing certain topics during online learning, where the median for topics avoided is three compared to six from the control group.

V. Summary

53 In response to our research questions, we find that interacting with commons resources helps inform students about the purpose of online learning and tutorial recordings. From our findings across both groups, students found the commons useful in supporting their data protection preferences. Some students in the control group would also have liked more information about how their data were being collected and used when being recorded.

54 The commons model is useful for supporting user preferences for protecting their personal data because it helps students develop a more detailed understanding of how their data are collected, used, and stored. Almost all participants consented to tutorial recording, indicating that students find value, both for

themselves and for the class overall, when it comes to being able to access a recording if needed. Most students also indicated factors such as accessibility and helping other students as reasons for consenting to recordings. While recording the level of consent can be useful in understanding whether participants feel comfortable with the collection of data for tutorial recordings, it only provides a limited picture as to the extent to which the ability to interact with the commons helps inform them about the purposes of online learning and tutorial recording. Therefore, it is important to consider other factors and means for understanding student agency when it comes to supporting their data protection preferences. Our approach in creating a commons for data protection also addresses the limits of the individualistic approach in the GDPR as we move away from using consent from understanding how tutorial recording and online learning impact students' education experiences.

55 More transparency around data protection between students, staff, university management, and other involved stakeholders is encouraged through a commons as the model supports the identification of stakeholder tensions and breaks them down through identifying a common aim: accessing a dynamic, participatory learning environment. The high levels of consent to tutorial recording could imply that students, to some extent, trust universities with their online learning data. However, given that more information on data protection was found to be preferable, students may want more details on how and what data are collected and used. This is particularly true in preventing potential harm should there be any data breaches, given the higher preference for understanding data protection and data subject rights. The commons model encourages more transparency around data protection between students and other stakeholders because it not only informs students of the data governance and risk management polices related to online learning data, but also supports recourse through data protection rights if any harms are realised.

56 More broadly, the commons model can be useful for reconsidering online learning pedagogies to support more inclusive and safe digital classrooms. Our results indicate that when asked about students' participation in recorded online tutorials compared to in-person sessions, most participants indicated that there would be topics that they would avoid discussing. This suggests that while students are happy to consent to tutorial recordings, they may decrease their level of participation in online classes. This could impact the quality of tutorial participation in online teaching. As a result, staff should be mindful of asking students questions related to their personal experience that may reveal these forms of data. Commons participants are also more willing to reveal their personal data, suggesting that an improved understanding of what and how data are collected and processed can encourage participation. Overall, staff and academic institutions should consider how the online learning environment could be fostered to maintain the privacy and security offered by the physical classroom.

G. Discussion

57 Our study found that a commons for online learning can support student agency as well as provide greater transparency on data protection regulations and the means to exercise their data protection rights.

58 As online learning continues, it is important that HEIs consider how students can be best informed about how their data are used. Given that students change their behaviour in online learning, only asking students to consent to being recorded without providing further information on their data is insufficient for ensuring student agency. Higher education data governance should be re-examined to reflect our changing digital learning environment, improving transparency and trust with the academic community.

I. Limitations

59 Our study has a number of limitations. Those who opted to participate are likely to be more privacy aware. Several participants mentioned that because data protection and tutorial recordings were mentioned in the study description, the thought was already on their mind beforehand. For unknown reasons, more students who identified as female participated in our study. Although we did not find any patterns or correlation to gender in response to our surveys, greater gender balance may be preferred to mitigate any potential biases.

60 Additionally, it was initially hoped that the study could have been done in groups to more accurately mimic the tutorial environment. However, challenges in recruiting participants, time zone difference, and asking them to spend more time on Microsoft Teams outside of classes meant that it was difficult to schedule participants to the same session. As a result, 28 students participated in the study individually and three pairs participated together. There was no identifiable difference between their responses.

61 Finally, we acknowledge that online learning during the pandemic is different to what it might have been if technologies were implemented more organically. Students, staff, and universities have had to instantly adapt to shifting the physical classroom into a digital one. The aim of our study is not to criticise HEIs for deploying technological solutions, but rather to encourage continued discussions on data protection considerations in education and suggest new socio-technical solutions that can help employ inclusive and innovative learning pedagogies to support the academic community.

II. Legal implications

62 According to the UK Higher Education Statistics Agency, there were 2.5 million students in higher education in the 2019/20 academic year,[81] where the vast majority of those students would have been online learning data subjects due to the pandemic. Despite the significant number, there is little attention given to improve support for how data in this sector should be used and protected.

63 While online learning safeguards are in place, as identified in Section B, many legal instruments and policies that can be applied to education are either general data protection principles or refer only to children's data. Although these are useful and should be followed by HEIs, they do not adequately deal with the complexities of online learning data that can impact students beyond education. In the UK, this was exemplified with the UK Office of Qualifications and Examinations Regulation (Ofqual) A-Levels grading algorithm scandal, where the regulatory body used an equation to calculate secondary school students' A-Levels results and therefore determined whether students were able to meet their university offers.[82] As the calculation heavily relied on the school's historical predicted grades and grade distribution, many pupils felt that their algorithmic result did not reflect their examination abilities, with long-term consequences that not only affected their higher education but subsequent careers. Students in higher education have also begun to fight back. Students from the University of Amsterdam,[83] University of

64 Maastricht,[84] City University of New York,[85] and University of Texas,[86] amongst many others, have organised petitions to push back against e-proctoring technologies not only because of privacy violations but also the technology's discriminatory nature and for fostering a surveillance-based academic environment. From our study, it is notable that students do care about what happens with their data, even if they trust institutions with it. As a result, in addition to the responsibility of providing education, HEIs should also have ethical responsibility to ensure that the use of student data by institutions themselves and third parties are actively communicated. This cannot be done through data protection alone and must include broader considerations of digital infrastructures and data governance strategies within higher education.

65 More broadly, wider conversations between data protection stakeholders could

81 Higher Education Statistics Authority, 'Who's studying in HE?' (9 February 2021) https://www.hesa.ac.uk/data-and-analysis/students/whos-in-he accessed 19 June 2022.

82 Alex Hern, 'Ofqual's A-level algorithm: why did it fail to make the grade?' (20 August 2020) https://www.theguardian.com/education/2020/aug/21/ofqual-exams-algorithm-why-did-it-fail-make-grade-a-levels accessed 19 June 2022.

83 Naomi Appelman, Jill Toh, and Hans de Zwart, 'Opinie: 'UvA, verhul racisme van proctoring niet met mooie woorden'' (6 July 2021) https://www.parool.nl/columns-opinie/opinie-uva-verhul-racisme-van-proctoring-niet-met-mooie-woorden~baa188f7/ accessed 19 June 2022.

84 Wendy Degens, 'Petition against online proctoring at the UM' (20 May 2020) https://www.observantonline.nl/english/Home/Articles/id/43194 accessed 19 June 2022.

85 Ian Ezinga, 'Student Petition Wins in Testing Software Fight' (28 October 2020) https://vanguard.blog.brooklyn.edu/2020/10/28/student-petition-wins-in-testing-software-fight/ accessed 19 June 2022.

86 Jason Kelley, 'Students Are Pushing Back Against Proctoring Surveillance Apps' (25 September 2020) https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps accessed 19 June 2022.

be facilitated to raise awareness on how personal data is being treated in our data-driven society within a data-protection focused data commons from legal, socio-technological, and ethical perspectives. This includes discussing the impact of data-related regulations and policies on data subjects. For example, within data protection regulations, access to the fundamental right to data protection through the exercise of data rights can be further strengthened.[87] Laws such as the European Data Governance Act[88] and Data Act[89] aims to increase trust in data intermediaries and strengthen data-sharing mechanisms across the EU, could support broader data protection practices for the benefit of data subjects outside of data protection. In the UK, from a group privacy perspective, *Lloyd v. Google*[90] raises interesting questions on collective action for privacy violation claims, which may lower the bar for collective redress actions.[91] Research and guidance from organisations and advisory bodies such as the Centre for Data Ethics and Innovation in the UK can play an important role connecting different stakeholders and addressing data issues to specific domains, including the data infrastructures needed to support a commons.[92] As a result, legal developments fostering the use of collaborative and co-created data-related practices can support greater fairness, accountability, and transparency on how data can be used for the benefit of individuals and groups. As students are becoming more aware of how online learning technologies use their personal data in and outside of classrooms, they have increasingly put pressure on HEIs to look beyond data protection considerations when deciding to adopt such technologies, focusing on the ethical, health, and wellbeing aspects of using educational data. Reiterating the limitations of consent from our study findings in Section F, it is important that matters beyond lawful basis of data processing are considered when it comes to how students can have agency over their online learning data and experience. This requires university management, data protection authorities, regulators, and policy makers to consider new ways in which online learning data should be regulated and governed to protect student data while also generating value for education.

III. Future work

66 Given that our online learning commons was only tested on students, further research could be done with staff to examine whether the commons could be useful for protecting their agency for protecting personal data. This is particularly important due to concerns of HEIs using educational technologies to monitor staff[93]and break union strikes,[94] where intellectual property rights do not always belong to the individual who produced the work.[95] With the rise of children's data collection in the classroom, the commons could also be tested on younger learners to examine its usefulness for students, teachers, and parents.

87 Jef Ausloos, Réne Mahieu, and Michael Veale, 'Getting Data Subject Rights Right A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance' (2020) 10(3) JIPITEC 283 https://nbn-resolving.de/urn:nbn:de:0009-29-50315.

88 European Union, 'Proposal for a Regulation of the European Parliament and of the Council onEuropean data governance (Data Governance Act)' (2021) 14606/21 Council of the European Union 1 https://data.consilium.europa.eu/doc/document/ST-14606-2021-INIT/en/pdf.

89 94 European Union, 'Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022) COM/2022/68 Council of the European Union 1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN.

90 UK Supreme Court, 'Lloyd v. Google' (2021) 50 UKSC 2019/0213 https://www.supremecourt.uk/cases/uksc-2019-0213.html.

91 Anuj Puri, 'The Group Right to Privacy' [2021] PhD Thesis 1 https://doi.org/10.17630/sta/161.

92 Centre for Data Ethics and Innovation, About Us (1 January 2018) https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about accessed 19 June 2022.

93 Evronia Azer, 'Remote working has led to managers spying more on staff – here are three ways to curb it' (6 May 2021) https://theconversation.com/remote-working-has-led-to-managers-spying-more-on-staff-here-are-three-ways-to-curb-it-159604 accessed 19 June 2022.

94 The Scotsman, 'Edinburgh University lecture recordings used against strikes' (7 March 2018) https://www.scotsman.com/education/edinburgh- university- lecture- recordings-used-against-strikes-332569 accessed 19 June 2022.

95 James Vincent, 'University staff are worried their recorded lectures will be used against them (20 August 2020) https://www.theverge.com/21373669/recorded-lecture-capture-copyright-universities-coronavirus-fears accessed 19 June 2022; 100 James Vincent, 'University staff are worried their recorded lectures will be used against them' (20 August 2020) https://www.theverge.com/21373669/recorded-lectur-capture-copyright-universities-coronavirus-fears accessed 19 June 2022.

67 As the commons aims to provide a socio-technical framework for increased protection and for expressing data protection preferences, it can be applied to other use cases both within online learning as well as other domains. For example, a data protection-focused data commons could be adopted for social media data archiving, where individuals may have preferences as to what, how, to whom, and for how long their posts are shared. Those who are part of the commons can also find out if there have been any recent scandals or data breaches related to different platforms. As the data protection-focused commons can be useful for demystifying the data protection regulations, policies, and processes for data subjects, future work can help identify new use cases for the benefit of communities across different sectors. Crucially, the application of the commons is not exclusive to countries that fall within the GDPR but can be tested in other jurisdictions to support a socio-technical means for greater student agency and data protection.

68 Beyond the commons, teaching pedagogies should be re-examined to ensure that students and staff are able to make the most of online learning technologies without losing some of the privacy and security offered by the in-person learning. More research could be done to examine whether student attitudes towards online learning has changed as they return to the in-person classroom. As students no longer have to fully rely on technology for academic study and are able to compare the online environment to in-person teaching, it can be expected that they are able to more accurately identify the benefits and downfalls of both.

69 More generally, given the rapid deployment of technologies to enable online learning delivery during the pandemic, there was understandably little time to explore how digital tools could be used to enhance learning within online education spaces. As a result, this period of digitisation may be characterised as a missed opportunity for co-creating teaching methods, forms, and pedagogies to support creative educational practices that extend and supplement physical classroom activities. To limit only replicating in-person educational norms using digital tools, as the impact of the pandemic eases, inclusive efforts to re-imagine the purpose of education and the role of technology through socio-technical lenses and education-related policies may help develop collaborative educational practices to support digital learning.

70 Considering the future development of the commons, to deploy a data commons in the long-term, considerations need to be made with regards to the platform used to host the commons and how the commons is to be sustained financially. While our study used Microsoft Teams, it does not represent the ideal platform for the commons. When deciding where and how the commons should be hosted, commons stakeholders should be involved in the decision-making process. Further work in this area could include developments on technical infrastructure and system considerations related to personal data, particularly whether the commons could be created within an existing digital ecosystem or built independently. Development decisions should be made in consultation with data subjects based on their accessibility, data, and data protection requirements, as well as expert advice to ensure that adequate checks and balances are in place to protect data that is processed within the commons. Given the difference in stakeholder interests, how and by whom the commons is maintained can impact the trust between users as data subjects and others participating in the commons' development.

H. Conclusion

71 In this paper, we set out to explore how and if a commons for online learning could support students' data protection preferences in a collaborative digital environment. As a result of the COVID-19 pandemic, universities and HEIs have rapidly deployed online learning technologies and tutorial recording, introducing new data-related harms. Although existing research and policy support more inclusive data governance practices within higher education institutions to reflect the increasingly digital academic landscape, the continuation of hybrid learning has prompted the need to create new solutions that help students maintain their agency over their personal data. Adopting existing commons and following good online learning practices, we suggest that a data protection-focused data commons can improve protecting students' personal data through co-creation and collaboration, placing their data protection preferences at the centre of the decision-making process. Our study builds, deploys, and tests a commons to assess whether its

collaborative resources help inform students about online learning purposes and if it can support their preferences for data protection. We found that although most students were not knowledgeable in university policies or data protection regulations, they consented to tutorial recordings. Beyond data protection, community and accessibility needs were noted reasons for consent. However, while the topic of the tutorial was found to have minimal impact on consent, if a tutorial is recorded, students may alter their behaviour and participation. Most students who tested the commons found that the resources were useful, particularly those related to data protection regulations and rights. This suggests that the commons can increase support for student preferences in protecting their personal data both *ex ante* and *ex post*, where greater transparency between students, university management, and use of data by online learning platforms can help students feel more assured about how their data are used and what recourse may be available should they have any data protection concerns. We suggest that consent as a means for informing students about tutorial recording is insufficient, where more research should examine student attitudes towards online learning as hybrid learning and the deployment of such technologies continue. The protection and governance of online learning data should go beyond data protection, as there are wider ethical and wellbeing considerations on how education technologies should be deployed. By applying a data protection-focused data commons for online learning, support for student agency over their personal data can be improved in a collaborative digital environment, helping them understand how their data are used by institutions and third-party organisations.

Appendix A: Adapting and applying the data protection IAD commons framework

72 To create a data protection-focused data commons for online learning, we applied the data protection IAD framework[96] for the use case of support students as data subjects in deciding and expressing their data protection preferences for online learning. The questions that were identified as part of the data protection IAD framework are answered as follows:

Background

73 The background context of the data protection-focused data commons for online learning involves the environment in which online learning is being undertaken and the requirement for tutorial recordings of that class. This was heightened by the COVID-19 pandemic that shifted all learning online.

- As online learning progressed, more awareness came to light about the monitoring of students through technologies. Pre-pandemic, there were also considerations about the impact of new technologies, tutorial and lecture recordings, and the digitisation of education more generally.

- Despite positive progress in containing the pandemic, institutions are continuing to adopt some of these technological practices even as in- person teaching is able to resume. As a result, it is important to ensure that students are able to understand how their data are used and have the ability to control that data.

74 As part of existing regulations such as the GDPR, universities and higher education institutions have the responsibility to clarify and explain how they use personal data. Currently, universities have privacy policies on online learning and tutorial recordings as well as wider data protection impact assessments and policies. Universities also have data protection officers as required by organisations of a certain size to respond to any data protection requests and answer and data protection related issues.

- Data protection-specific and sector-wide organisations include the ICO, JISC, and the Office for Students that outline what and how data should and should not be used in relation to the work environment and specifically for higher education. Some of this work pre-dates the COVID-19 pandemic and some research was published during the pandemic in producing solutions that support the protection of personal data for the future of education.

96 Michael D McGinnis, 'The IAD Framework in Action: Understanding the Source of the Design Principles in Elinor Ostrom's Governing the Commons' in Daniel Coleand and Michael D McGinnis (eds), Elinor Ostrom and the Bloomington School of Political Economy, Volume 3: A Framework for Policy Analysis (Lexington 2018) https://polisci.indiana.edu/documents/profiles/mcginnis1.pdf.

- Students' personal data are separate from other forms of data that universities manage. For example, students' administrative data, examination and assessments data, and data from tutorials are all managed differently by different departments within the university. However, there may be some overlap, highlighting the importance of students being able to control and understand how their personal data from tutorials are being process. Universities generally follow FAIR data principles with regards to research data.

- Students may not be aware of how their institution managed their data and may not feel like they can challenge their institution given that doing so could negatively impact both their academic experience as well as their grades.

- Trust issues between students and their institutions, as well as staff and their institutions, may have arisen based on incidences of technology adoption as well as sharing of recordings without explicit consent.

Data Attributes

75 The data and personal data that are part of the commons.

- Student's personal data as part of Microsoft Teams such as student ID, the content they reveal in the tutorial, chat data, screen sharing, and their voice.

- If they disclose any disabilities, racial information, religious information, political identities, or union membership, this could be classified as sensitive data.

- The data is collected and processed following universities' policies, through Microsoft Teams, and possibly internationally if the student is not based within the UK.

- University and third party software collect, store, and process the data.

- The data is stored privately although tutorial recordings may be shared with other students. Currently, students have limited control as to whether they want to be recorded.

- University tutors, IT teams, and systems teams are responsible for how the data is stored, shared, and retained, with different administrative privileges.

- The university uses third party software such as Microsoft Teams as well as Panopto to record and store recordings.

- Students have limited control and authority in the process. They only have information of the university policies.

- Some of the risks include extensive data gathering unrelated to education, potential discrimination from e-proctoring software, and creating a surveillance academic environment.

Commons Community Members

76 The commons aims to support students and will also include staff, IT admin, and potential experts or those who are able to provide external advice outside of the university.

77 The commons is only relevant for those within the university community given that the data only applies to online learning.

78 The technology companies that provide the tools for online learning as well as higher education organisations such as JISC or the OfS may be relevant for the commons.

79 Students have a power imbalance between themselves, staff, and the university management given that if they refuse certain personal data to be collected or provided, they may not be able to access education, with negative impact on their academic prospects.

Goals and Objectives

80 The objective of the commons is to support students' online learning personal data preferences and help them understand what data protection rights and recourse they have should they not want their personal data to be used in certain ways.

Managing and Governing the Commons

81 The commons will sit in top of the online learning platform, in this case Microsoft Teams, to allow seamless and integrated access to the tool while not compromising their privacy with respect to others in the tutorial.

- The commons will allow students to choose whether they want to consent to tutorial recording both before and after the tutorial, with respect to the collection and processing of their personal data in that way.

- Online learning data that is collected is

shared within the tutorial and possibly to other students as well, where the recording may be re-purposed for teaching beyond the session in which the student participated in.

- No data protection mechanisms currently exist for this use case and only university policies are applied.
- The relevant data subject rights include the right of access, the right to data portability, and the right to object to automated decision-making.
- Purpose limitation may have been considered but is inconclusive.

82 Determine the governance mechanisms of the commons.

- The commons community consists of those who are affiliated with the university.
- There is no requirement for those who participate to share their personal data or their experience, but in order for the commons to function to meet its aims, students need to vote as to whether they consent to tutorial recording.
- If appropriate, the tutor can mitigate any issues. If not, then an external, neutral expert can help as well as addressing the data protection officer.
- Existing platforms that are used to conduct online learning may be updated with more privacy support or offer tools that can improve the protection of users' personal data.

83 Identifying decision makers and experts.

- External experts can be identified to support the commons, such as academic from other institutions, privacy professionals, and independent or international higher education bodies.

84 Decision-making on the commons is determined in part by the tutor, the department, and university management, with the latter making the most impact.

- The commons would be digital and take place on the same platform as where the online learning is taking place.
- Some of the infrastructure is internal, for example where the recording may be embedded and uploaded. Some of the infrastructure is external and provided by third party companies.

85 Establishing formal or informal norms that govern the commons.

- The commons follows the same guidelines as the terms of service of the online learning provider as well as university policies.
- Students and the commons community can provide feedback on their online learning experience through standard university procedures.
- Some institutions, such as the Open University, have greater experience with delivering online learning.

Outcomes

86 Benefits of the commons.

- Students are able to increase their understanding and control of how their personal data are being used as well as what avenues there are to object against some sues of personal data.
- The commons community should expect advice and guidance on what is allowed, as well as the ability to anonymously share their experience with others.

87 Costs and risks of the commons.

- The commons has minimum risk given that no extra personal data are being collected. There are mechanisms in place to ensure that their consent vote is anonymous and cannot be traced back to them or the tutor. There are no risks of further data breaches or privacy problems.
- As the tool is developed on Microsoft Teams and hosted by internal university servers, there are no additional risks from the data infrastructure.
- The rights available under the GDPR apply to the commons where applicable to personal data

Appendix B: Mock-Tutorial Instructions

88 As part of the Online Learning as a Commons study, we would like you to imagine that you are participating in a Teams-based tutorial. If you have not yet received a Teams meeting

invitation, please e-mail the researchers.

89 Please read the tutorial scenario below. Note that no further preparation will be needed before the Teams meeting.

Tutorial: An Introduction to Conducting Research on Social Media

90 In our digitally connected society, social media such as Facebook, Twitter, LinkedIn, and Instagram are used not only for sharing parts of our lives with others, but also used by businesses, event organisers, recruiters, and data brokers to understand how individuals and groups interact.

91 In this introduction, we will explore the types of data that are collected through social media, different techniques for conducting social media research, and review some examples and case studies.

92 This tutorial is aimed at a general audience and is suitable for all disciplines.

93 **1.** What is social media research? Social media research is where quantitative or qualitative data is being gathered from social networking sites (SNS). This research can be done in many forms. Examples of social media research include:

- Downloading tweets from the Twitter Archive and looking at specific hashtags.
- Looking at the user engagement (such as views, clicks, and location) of an advertisement put out by a business on Facebook.
- Creating polls on Instagram and asking users specific questions.

94 Social media research can be conducted by individuals and businesses to understand specific demographics of users to serve them specific content or find out more about their behaviours.

95 Questions:

- Can you think of other examples of social media research?
- Have you participated in social media research?
- What are other purposes of conducting social media research?

96 **2.** How can we conduct social media research ethically? Given the pervasiveness of social media and data on SNS, it has become much easier to conduct research on social media. However, this means that there may be less checks and balances when it comes to conducting research ethically. Traditional means of ensuring that research is ethical may not be applicable to the digital environment. For this part of the tutorial, we will discuss the challenges of conducting research on social media more generally.

97 Questions:

- To what extent do you think conducting ethical research from social media may be different to ethical research more generally?
- Given that formal ethics applications and consent procedures may not work for social media research, what do you think are possible solutions for conducting such research?
- Do you think conducting ethical research can help ensure that social network data are gathered in more ethical ways?

98 **3.** Guidance for conducting social media research For the final part of the tutorial, we will look at guidance for conducting social media research. We will read excerpts from the University's social media research ethical guidance as well as external policies that support ethical research.

99 Questions:

- What do you think about the guidance and policies that we read? Are they useful for researchers or for participants?
- What other things do you think should be included in social media research ethical guidance and policies?
- Do you think guidance and policies are enough to ensure that social media research is conducted ethically?

100 If you are interested in the content of the tutorial, please find a few resources below:

- "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" Carole Cadwalladr and Emma Graham-Harrison, The Guardian.
- "Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts" edited by Michael

Zimmer and Katharina Kinder-Kurlanda.

- University social media research ethical guidance

Appendix C: Adapted IUIPC questions

101 The following statements are IUIPC questions adapted for online learning included in the final survey of the study. The statements were presented in Likert matrices with five responses available, ranging from strongly disagree to strongly agree.

102 The following statements relate to privacy practices:

- Online learning platforms should disclose the way my personal data are collected, processed, and used.
- Universities should disclose the way my personal data are collected, processed, and used.
- It is very important to me that I am aware and knowledgeable about how my personal information will be used.

103 The following statements relate to control over your personal data:

- Users' online privacy is really a matter of users' right to exercise control over how their information is collected, used, and shared.
- I believe that online privacy is violated when control over how users' information is collected, used, and shared is lost.

104 The following statements relate to data collection:

- It bothers me when online learning platforms ask me for personal information.
- It bothers me when universities ask me for personal information.
- When online learning platforms ask me for personal information, I sometimes think twice before providing it.
- When universities ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.